Tenable.io Report

Tenable.io Report

Wed, 09 Nov 2022 13:39:38 UTC

Table Of Contents

Vulnerabilities By Host

formacionssf.didacsis.com

Scan Information

Start time:	2022/11/09 13:06
End time:	2022/11/09 13:39

Host Information

DNS Name:	formacionssf.didacsis.com
OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	6	4	63	75

Results Details

/

72779 - DNS Server Version Detection

Synopsis

Nessus was able to obtain version information on the remote DNS server.

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.
Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0937

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2014/03/03, Modification date: 2020/09/22

Ports

formacionssf.didacsis.com (TCP/53) Vulnerability State: Active

```
DNS server answer for "version.pdns" (over TCP) :

  PowerDNS Authoritative Server 4.4.1 (built May 12 2022 16:30:11 by root@bh-
centos-7.dev.cpanel.net)
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

See Also

Solution

Protect your target with an IP filter.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/02/04, Modification date: 2022/08/15

Ports

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
Port 2087/tcp was found to be open
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
Port 465/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
Port 2078/tcp was found to be open
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
Port 21/tcp was found to be open
```

formacionssf.didacsis.com (TCP/111) Vulnerability State: Active

```
Port 111/tcp was found to be open
```

formacionssf.didacsis.com (TCP/53) Vulnerability State: Active

```
Port 53/tcp was found to be open
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

```
Port 143/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
Port 2091/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
Port 2083/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2086) Vulnerability State: Active

```
Port 2086/tcp was found to be open
```

formacionssf.didacsis.com (TCP/587) Vulnerability State: Active

```
Port 587/tcp was found to be open
```

formacionssf.didacsis.com (TCP/3306) Vulnerability State: Active

```
Port 3306/tcp was found to be open
```

formacionssf.didacsis.com (TCP/389) Vulnerability State: Active

```
Port 389/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
Port 2096/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2079) Vulnerability State: Active

```
Port 2079/tcp was found to be open
```

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

```
Port 110/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2095) Vulnerability State: Active

```
Port 2095/tcp was found to be open
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: Active

```
Port 993/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2077) Vulnerability State: Active

```
Port 2077/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2082) Vulnerability State: Active

```
Port 2082/tcp was found to be open
```

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
Port 22/tcp was found to be open
```

formacionssf.didacsis.com (TCP/25) Vulnerability State: Active

```
Port 25/tcp was found to be open
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
Port 2080/tcp was found to be open
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
Port 443/tcp was found to be open
```

formacionssf.didacsis.com (TCP/995) Vulnerability State: Active

```
Port 995/tcp was found to be open
```

formacionssf.didacsis.com (TCP/80) Vulnerability State: Active

```
Port 80/tcp was found to be open
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2003/12/09, Modification date: 2022/03/09

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

```
Remote operating system : Linux
Confidence level : 59
Method : SinFP


The remote host is running Linux
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2006/06/05, Modification date: 2022/07/25

Ports

formacionssf.didacsis.com (TCP/995) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
 SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
 SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
```

```
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA [...]
```

formacionssf.didacsis.com (TCP/389) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     --------------------
---
   DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     --------------------
---
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   IDEA-CBC-SHA                  0x00, 0x07       RSA           RSA      IDEA-CBC(128)
SHA1
   RC4-MD5                       0x00, 0x04       RSA           RSA      RC4(128)
MD5
   RC4-SHA                       0x00, 0x05       RSA           RSA      RC4(128)
SHA1
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
SHA1
   RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
SHA256


SSL Version : TLSv11
  Medium Strength Ciphers (> 64-bit and < 112-bit [...]
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.
```

```
SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
```

```
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
SHA1
   AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA      RC4(128)
SHA1
   AECDH-AES128-SHA              0xC0, 0x18       ECDH          None     AES-CBC(128)
SHA1
   AECDH-AES256-SHA              0xC0, 0x19       ECDH          None     AES-CBC(256)
SHA1
   AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None     RC4(128)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA     [...]
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
```

```
   ----------------------        ----------       ---           ----     ---------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384

The fields above are :
```

```
  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01       -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03       -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH          RSA      ChaCha20-Poly1305(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
```

```
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
 MAC
   ----------------------        ----------       ---           ----     --------------------
 ---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}

Note that this service does not encrypt traffic by default but does
support upgrading to an encrypted connection using STARTTLS.
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
 MAC
   ----------------------        ----------       ---           ----     --------------------
 ---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
```

```
MAC={message authentication code}
{export flag}
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/12/01, Modification date: 2021/02/03

Ports

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/389) Vulnerability State: Active

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
This port supports TLSv1.3/TLSv1.2.
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/995) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

```
This port supports TLSv1.2.
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
This port supports TLSv1.2.
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/08/19, Modification date: 2022/07/26

Ports

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
A TLSv1.2 server answered on this port.

A web server is running on this port through TLSv1.2.
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
A TLSv1.2 server answered on this port.

A web server is running on this port through TLSv1.2.
```

formacionssf.didacsis.com (TCP/25) Vulnerability State: Active

```
An SMTP server is running on this port.
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
An FTP server is running on this port.
```

formacionssf.didacsis.com (TCP/3306) Vulnerability State: Active

```
A MariaDB server is running on this port.
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
A TLSv1.2 server answered on this port.

An SMTP server is running on this port through TLSv1.2.
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
A TLSv1.2 server answered on this port.

A web server is running on this port through TLSv1.2.
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

A TLSv1.2 server answered on this port.

A web server is running on this port through TLSv1.2.

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

A TLSv1.2 server answered on this port.

A web server is running on this port through TLSv1.2.

formacionssf.didacsis.com (TCP/995) Vulnerability State: Active

A TLSv1.2 server answered on this port.

A POP3 server is running on this port through TLSv1.2.

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

An SSH server is running on this port.

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

A TLSv1.2 server answered on this port.

A web server is running on this port through TLSv1.2.

formacionssf.didacsis.com (TCP/80) Vulnerability State: Active

A web server is running on this port.

formacionssf.didacsis.com (TCP/993) Vulnerability State: Active

A TLSv1.2 server answered on this port.

An IMAP server is running on this port through TLSv1.2.

formacionssf.didacsis.com (TCP/587) Vulnerability State: Active

An SMTP server is running on this port.

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

An IMAP server is running on this port.

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

A POP3 server is running on this port.

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

A TLSv1.2 server answered on this port.

A web server is running on this port through TLSv1.2.

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

See Also

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

2.5

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

1.9 (E:U/RL:OF/RC:C)

References

CVE	CVE-2008-5161
BID	32319
XREF	CWE:200
XREF	CERT:958563

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2013/10/28, Modification date: 2018/07/30

Ports

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.
Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.
Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?ae636e78

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	33065
BID	11849
XREF	CWE:310

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2016/12/08, Modification date: 2022/10/12

Ports

formacionssf.didacsis.com (TCP/2087) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
```

```
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
```

```
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
```

```
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/995) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
```

```
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

formacionssf.didacsis.com (TCP/110) Vulnerability State: New

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate
 Services
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Jan 01 00:00:00 2004 GMT
Valid To            : Dec 31 23:59:59 2028 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQ
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDK
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r
+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yq
+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/05/04, Modification date: 2020/05/04

Ports

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/389) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/995) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

166602 - Asset Attribute: Fully Qualified Domain Name (FQDN)

Synopsis

Report Fully Qualified Domain Name (FQDN) for the remote host.

Description

Report Fully Qualified Domain Name (FQDN) for the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/10/27, Modification date: 2022/10/27

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: New

```
The FQDN for the remote host has been determined to be:

  FQDN       : 6050329.didacsis.com
  Confidence : 100
  Resolves   : True
  Method     : rDNS Lookup: IP Address

Another possible FQDN was also detected:
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.
Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2000/04/28, Modification date: 2022/06/17

Ports

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
The following string will be used :
TYPE="password"
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
The following string will be used :
TYPE="password"
```

formacionssf.didacsis.com (TCP/80) Vulnerability State: Active

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :
```

```
http://formacionssf.didacsis.com/PlCaU2kSwpUf.html
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
The following string will be used :
TYPE="password"
```

20870 - LDAP Server Detection

Synopsis

An LDAP server was detected on the remote host.

Description

The remote host is running a Lightweight Directory Access Protocol (LDAP) server. LDAP is a protocol for providing access to directory services over TCP/IP.

See Also

https://en.wikipedia.org/wiki/LDAP

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2006/02/10, Modification date: 2022/09/29

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

6.1

CVSS v3.0 Base Score

7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS Base Score

5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-2016-2183

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/11/23, Modification date: 2021/02/03

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA       3DES-CBC(168)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: New

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA       3DES-CBC(168)
SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17        ECDH          None      3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA       3DES-CBC(168)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: New

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA       3DES-CBC(168)
SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA       3DES-CBC(168)
SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17        ECDH          None      3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA       3DES-CBC(168)
SHA1

The fields above are :

  {Tenable ciphername}
```

```
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/12/07, Modification date: 2021/03/09

Ports

formacionssf.didacsis.com (TCP/2091) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption
 MAC
    ----------------------        ----------        ---           ----      --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA       AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)
```

```
   Name                          Code            KEX          Auth     Encryption
MAC
   ----------------------        ----------      ---          ----     --------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E      DH           RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F      DH           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F      ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30      ECDH         RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/995) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

   Name                          Code            KEX          Auth     Encryption
MAC
   ----------------------        ----------      ---          ----     --------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E      DH           RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F      DH           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F      ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30      ECDH         RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

   Name                          Code            KEX          Auth     Encryption
MAC
   ----------------------        ----------      ---          ----     --------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E      DH           RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F      DH           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F      ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30      ECDH         RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
```

```
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
    DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     --------------------
 ---
```

```
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384

The fields above are :

 {Tenable ciphername}
 {Cipher ID code}
 Kex={key exchange}
 Auth={authentication}
 Encrypt={symmetric encryption method}
 MAC={message authentication code}
 {export flag}
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH            RSA      3DES-CBC(168)
SHA1
   ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
SHA1

 High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH            RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH            RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH          RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH          RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH            RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH            RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH            RSA      SEED-CBC(128)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA      RC4(128)
SHA1
   DHE-RSA-AES128-SHA256   [...]
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

 High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
```

```
   ----------------------        ----------       ---          ----     --------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH           RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH         RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8       ECDH         RSA      ChaCha20-Poly1305(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/110) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX          Auth     Encryption
MAC
   ----------------------        ----------       ---          ----     --------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH           RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH         RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX          Auth     Encryption
MAC
   ----------------------        ----------       ---          ----     --------------------
---
   DHE-RSA-AES128-SHA256         0x00, 0x9E       DH           RSA      AES-GCM(128)
SHA256
   DHE-RSA-AES256-SHA384         0x00, 0x9F       DH           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDH         RSA      AES-GCM(128)
SHA256
   ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDH         RSA      AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

```
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    DHE-RSA-AES128-SHA256         0x00, 0x9E        DH            RSA       AES-GCM(128)
SHA256
    DHE-RSA-AES256-SHA384         0x00, 0x9F        DH            RSA       AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: New

```
Here is the list of SSL PFS ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA       3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F        ECDH          RSA       AES-GCM(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30        ECDH          RSA       AES-GCM(256)
SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA       AES-CBC(256)
SHA1
    ECDHE-RSA-RC4-SHA             0xC0, 0x11        ECDH          RSA       RC4(128)
SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27        ECDH          RSA       AES-CBC(128)
SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28        ECDH          RSA       AES-CBC(256)
SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
```

```
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

http://www.isg.rhul.ac.uk/tls/

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.nessus.org/u?ac7327a0

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

https://www.rc4nomore.com/

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

Vulnerability Priority Rating (VPR)

3.6

CVSS v3.0 Base Score

5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.4 (E:U/RL:X/RC:C)

CVSS Base Score

4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

3.7 (E:U/RL:ND/RC:C)

References

CVE	CVE-2013-2566
CVE	CVE-2015-2808
BID	73684
BID	58796

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2013/04/05, Modification date: 2021/02/03

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth      Encryption
 MAC
    ----------------------        ----------       ---           ----      --------------------
 ---
    RC4-MD5                       0x00, 0x04       RSA           RSA       RC4(128)
 MD5
    RC4-SHA                       0x00, 0x05       RSA           RSA       RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: New

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth      Encryption
 MAC
    ----------------------        ----------       ---           ----      --------------------
 ---
    ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA       RC4(128)
 SHA1
    AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None      RC4(128)
 SHA1
    RC4-MD5                       0x00, 0x04       RSA           RSA       RC4(128)
 MD5
    RC4-SHA                       0x00, 0x05       RSA           RSA       RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: New

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth      Encryption
 MAC
    ----------------------        ----------       ---           ----      --------------------
 ---
    ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH          RSA       RC4(128)
 SHA1
    AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None      RC4(128)
 SHA1
    RC4-MD5                       0x00, 0x04       RSA           RSA       RC4(128)
 MD5
    RC4-SHA                       0x00, 0x05       RSA           RSA       RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

```
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

100669 - Web Application Cookies Are Expired

Synopsis

HTTP cookies have an 'Expires' attribute that is set with a past date or time.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, Nessus has detected that one or more of the cookies have an 'Expires' attribute that is set with a past date or time, meaning that these cookies will be removed by the browser.

See Also

https://tools.ietf.org/html/rfc6265

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.
If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/06/07, Modification date: 2021/12/20

Ports

formacionssf.didacsis.com (TCP/80) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
```

```
Port :


Name : Horde
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

```
Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

```
Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

```
Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
```

```
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

```
Name : Horde
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
```

```
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
```

```
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
```

```
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
```

```
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
```

```
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
```

```
Comment :
Secure : 0
Httponly : 1
Port :
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
The following cookies are expired :

Name : roundcube_sessauth
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : PPA_ID
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : horde_secret_key
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /
Value : expired
Domain : .formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : imp_key
Path : /
Value : expired
Domain : formacionssf.didacsis.com
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : cprelogin
Path : /
Value : no
Domain :
Version : 1
```

```
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : roundcube_sessid
Path : /
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : whostmgrrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : webmailrelogin
Path : /
Value : no
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : Horde
Path : /horde
Value : expired
Domain :
Version : 1
Expires : Thu, 01-Jan-1970 00:00:01 GMT
Comment :
Secure : 0
Httponly : 1
Port :
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/05/19, Modification date: 2021/02/03

Ports

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
 Subject Name:

Common Name: 6050329.didacsis.com

Issuer Name:

Country: US
State/Province: TX
Locality: Houston
Organization: cPanel, Inc.
Common Name: cPanel, Inc. Certification Authority

Serial Number: 00 F1 93 B4 87 D7 95 1C C1 EE DB 22 01 58 E4 BC 27

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 17 00:00:00 2022 GMT
Not Valid After: Nov 15 23:59:59 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 BF 73 EB 6F 84 1C D9 54 39 F2 DE 58 FA 1E 61 C6 28 B0 BF
            87 84 3C 66 9C 4A 20 BE 28 42 5B B8 0E 6A B4 95 87 0F F9 70
            54 4F 51 9C 4D 09 F4 00 30 47 55 96 25 11 02 EA 4B 3F 7A 0B
            9C CC 39 C1 79 B9 B8 8F BC 84 EE 57 5E 87 87 87 F8 4B 68 5B
            05 E7 C8 83 7C 82 4D 82 A2 DC 6A 98 B4 28 B7 EF B6 BA 49 42
            B6 35 BF B5 9C 6B 08 92 88 F5 9D FA 6F BD 4C 1E 10 16 65 D8
            C6 14 CA 13 0C 07 83 F1 4A 18 C5 6F 95 73 A2 2C B6 E9 0B 16
            3F 3B 0B EA D1 D2 B4 8C 4C 52 74 DA BD 8C 4C 88 42 B0 94 10
            08 33 C9 0A D7 62 56 21 B0 4A B9 E0 02 54 D5 DD 5D 41 C1 39
            51 5A AF 15 29 50 AF 1C 33 D0 99 1B 68 40 CB 09 4F FC AB 44
            9D 9A E9 5F FB DF 44 62 5C 87 24 5C 5F 8A 52 8F 3A 53 FA 97
            E3 EE 4E F8 D1 E4 26 76 10 B8 85 59 75 22 00 3C EA 79 49 C9
            47 80 71 59 8E 6C CD 23 71 EF AF 96 A3 BF B7 02 21
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 3B 72 1F BC 02 E9 6A 48 A2 C5 FC 6B B1 94 AB A9 FD 8B D7
           D3 A1 64 44 62 20 34 E0 62 01 FC 07 BE D7 EA 71 9F 29 F0 BD
           85 E5 ED 29 5C 77 4E BB 74 D9 F8 94 97 4B 3B B2 66 F1 AC 22
           BA 62 4A 69 88 A3 E0 62 C0 1C 6D 62 F6 37 54 E4 FC D9 3A 1C
           A1 54 0A 27 DB D1 C5 BF 86 62 66 2B 47 58 19 D4 99 D1 63 81
           F2 4F 24 A6 17 85 55 8D 03 C1 EC 4A EE 9F 56 17 56 F0 0A ED
           D8 87 41 2A F8 FF 47 11 85 D4 C1 3A A9 9C E4 0E 49 45 A7 71
           2E 2E CA 12 C8 2C 67 87 18 82 33 E5 D0 B9 1B 52 69 2E [...]
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption
```

```
Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
```

```
            03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
            94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
            AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
            CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
            4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
            53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
            75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/389) Vulnerability State: Active

```
 Subject Name:

Common Name: 6050329.didacsis.com

Issuer Name:

Common Name: 6050329.didacsis.com

Serial Number: 00 BD 17 D4 6F

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Sep 15 22:19:27 2022 GMT
```

```
Not Valid After: Sep 15 22:19:27 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 BB A9 92 10 5E F9 82 B2 A2 D2 DA 9D 81 21 B0 E4 E8 57 DB
            25 25 F0 5C 65 78 41 E2 73 94 69 35 5C C6 A1 F4 94 E6 F8 34
            D7 9F 31 9F 7E B9 7D 4A 6F A9 62 75 34 C8 90 0E E6 60 9A DF
            54 E6 5D 5E B5 AD 55 85 97 A0 E1 74 8F C2 61 EE 3C 55 EB A8
            10 0F 3E C1 E7 8C A3 A0 0F F8 86 CC F6 F3 14 D2 F3 0D 40 D1
            93 C5 55 D3 98 A6 71 C1 FA B3 EC CA 75 11 0D 88 86 F2 C4 18
            84 23 3E 9C F8 5D A5 C4 3D
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 B1 2C 2E B3 35 80 1C 71 94 62 7A CF 4B E7 EE DE 65 FF B1
           2D D1 A1 55 D0 C8 63 C7 00 C7 B7 BE CA 63 06 B0 5D 33 3A BC
           7F B9 FE 1B A6 24 24 9D AE 2C 62 C2 5E 36 3A B7 AE BE DC 4E
           BD F6 39 99 ED 79 FF DB E6 5A 04 C7 87 4E CF 55 C8 CD 70 A1
           41 B2 18 62 D8 0C 73 2E 40 D4 0A 9D 39 FF E9 9B 7B 17 87 5D
           60 50 34 A1 B5 31 14 8A 91 E2 10 1E 14 3D F4 C8 7B B1 8A 2B
           3A 91 1F DE E3 77 6B 7A 50

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: 6050329.didacsis.com
DNS: localhost
DNS: localhost.localdomain


Fingerprints :

SHA-256 Fingerprint: 89 E0 12 EE 4D 37 22 0D 9F 79 3F E9 14 A1 E7 4B 1A 8C 3C B2
                     3D 87 76 B0 39 6E 1B F5 BE 95 1D BE
SHA-1 Fingerprint: 10 06 40 C8 99 AA 09 C4 1E 04 13 50 69 FB 1F AA 69 40 6C BD
MD5 Fingerprint: 69 AA 5F 93 3D 11 2C 0F 14 12 2D 59 BB 8E 4B C8


PEM certificate :

-----BEGIN [...]
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
```

```
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com
```

```
Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
```

```
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
 Subject Name:
```

```
Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
```

```
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

formacionssf.didacsis.com (TCP/995) Vulnerability State: Active

```
 Subject Name:

Common Name: *.didacsis.com

Issuer Name:

Country: GB
State/Province: Greater Manchester
Locality: Salford
Organization: Sectigo Limited
Common Name: Sectigo RSA Domain Validation Secure Server CA

Serial Number: 00 C2 AB 8F 39 63 DF B2 5C D3 10 D3 24 7D 7A E8 CF

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Nov 03 00:00:00 2022 GMT
Not Valid After: Nov 03 23:59:59 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A4 54 63 3F DB BD E1 C1 6F 35 6B 2D 45 6C E8 66 2B 0C D5
            2E 39 09 1F 15 F1 B6 78 15 7B 56 1B 8C B2 33 3F CE 45 F9 E5
            0A DC 7A 9B 3D D1 67 E3 ED 19 DA 16 3C ED 79 77 EB 87 EA 45
            58 1E 79 36 22 07 E3 E7 FF 4C C8 23 23 DF E5 71 B4 C0 53 4F
            67 FB 72 73 6B 32 4D 8C 4E 11 1C 0D 2E 17 7B 56 92 BF 01 64
            F9 32 CD F5 43 61 FD BC 3D C0 D5 52 E8 43 85 ED 70 89 16 B7
            8E 47 ED 17 06 72 AF 0F 5C A3 DD D5 FD 4A 1D 79 D6 24 5B 2B
            66 D1 EB CB DD 4B 4E 70 A3 10 2B E0 17 78 B5 C2 09 94 50 8F
            CD 5C D5 84 67 59 AB A1 3E 25 E9 F0 42 48 20 52 82 0B 03 8F
            05 57 62 E3 EB 99 90 42 9F 9A EE 0A C7 B6 BB 49 4F 78 05 A2
            9C E1 B0 5E 2B BB 14 96 07 66 2C 61 32 FC 38 BE E2 07 46 29
            3F 08 71 FC DA EF 13 B5 05 5E 02 93 5B 9F 22 29 7A 14 AB A7
            A3 5F D9 D8 66 C2 3F 73 2D AE A1 37 E0 53 F9 3A AD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 50 35 6B AD 03 FB 69 45 74 53 B1 69 B4 30 C4 B4 D4 87 6B
           03 83 45 EC EF 11 67 0A A2 DC 1C 0F 7B 3C E8 7D 32 E2 1F 8B
           94 BC 3C 1A DC A5 72 6D CA 1A DB 76 B8 F5 65 29 89 C2 B5 5B
           AD 40 A1 3F EA D1 40 0D C4 DF 8D B7 32 7F 4A 6F 0C D3 A8 31
           CD AE A2 7B 4C F1 06 89 BA 48 26 47 D0 B8 01 2D 77 D2 51 23
           4B 19 61 F6 EA 5E BC EB ED 9C BC 38 7D 9B 8A 22 A5 1B 8F E9
           53 62 C6 CA 17 7D 9D 0D 67 F0 4B 44 D1 A7 D2 A4 B3 F2 F7 8E
           75 C8 A0 0E 48 2C 47 3C 29 D1 [...]
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/01/30, Modification date: 2019/11/22

Ports

formacionssf.didacsis.com (TCP/2078) Vulnerability State: New

```
Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : OPTIONS, PROPFIND, GET, LOCK, MKCOL, COPY, PROPPATCH, MOVE, DELETE, UNLOCK,
 HEAD, PUT, POST
Headers :

  Date: Wed, 09 Nov 2022 13:27:25 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: formacionssf.didacsis.com:2078
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Restricted Area"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

<html>Authorization Required</html>
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: New

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Wed, 09 Nov 2022 13:27:28 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: cprelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: cpsession=%3ao1UWL3IZbPx7SmRQ%2c36bd8db61927fd9e30ab19ff41931b5a; HttpOnly; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2083; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2083; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2083;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=formacionssf.didacsis.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2083; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2083
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2083
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Frame-Options: SAMEORIGIN
  X-Content-Type-Options: nosniff
  Content-Length: 32171
```

```
Response Body :


<!DOCTYPE html>
<html lang="en" dir="ltr">
<head>
   [...]
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: New

```
Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Wed, 09 Nov 2022 13:27:26 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: formacionssf.didacsis.com:2080
  Cache-Control: no-cache, no-store, must-revalidate, private
  Connection: close
  Vary: Accept-Encoding
  WWW-Authenticate: Basic realm="Horde DAV Server"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"
  Expires: Fri, 01 Jan 1990 00:00:00 GMT

Response Body :

<html>Authorization Required</html>
```

formacionssf.didacsis.com (TCP/2096) Vulnerability State: New

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Wed, 09 Nov 2022 13:27:33 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: webmailrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: webmailsession=%3aB2mO5nZua38NgNXy%2c1f342b79b423e8caddf03093e0887605; HttpOnly;
 path=/; port=2096; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2096; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2096; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2096;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=formacionssf.didacsis.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2096; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2096
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2096
  Set-Cookie: roundcube_cookies=enabled; HttpOnly; expires=Thu, 09-Nov-2023 13:27:32 GMT; path=/;
 port=2096; secure
```

```
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Frame-Options: SAMEORIGIN
  [...]
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: New

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Content-Type: text/html; charset="utf-8"
  Date: Wed, 09 Nov 2022 13:27:29 GMT
  Cache-Control: no-cache, no-store, must-revalidate, private
  Pragma: no-cache
  Set-Cookie: whostmgrrelogin=no; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
  Set-Cookie: whostmgrsession=%3andrZFOU04ep6bVnJ%2c58a256f38a0f5c16cf5a98dd732c9f7b; HttpOnly;
 path=/; port=2087; secure
  Set-Cookie: roundcube_sessid=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/;
 port=2087; secure
  Set-Cookie: roundcube_sessauth=expired; HttpOnly; domain=formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
  Set-Cookie: Horde=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/horde;
 port=2087; secure
  Set-Cookie: PPA_ID=expired; HttpOnly; expires=Thu, 01-Jan-1970 00:00:01 GMT; path=/; port=2087;
 secure
  Set-Cookie: imp_key=expired; HttpOnly; domain=formacionssf.didacsis.com; expires=Thu, 01-
Jan-1970 00:00:01 GMT; path=/; port=2087; secure
  Set-Cookie: Horde=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu, 01-Jan-1970
 00:00:01 GMT; path=/; port=2087
  Set-Cookie: horde_secret_key=expired; HttpOnly; domain=.formacionssf.didacsis.com; expires=Thu,
 01-Jan-1970 00:00:01 GMT; path=/; port=2087
  Cache-Control: no-cache, no-store, must-revalidate, private
  X-Frame-Options: SAMEORIGIN
  X-Content-Type-Options: nosniff
  Content-Length: 31838

Response Body :


<!DOCTYPE html>
<html lang="en" [...]
```

formacionssf.didacsis.com (TCP/80) Vulnerability State: New

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Wed, 09 Nov 2022 13:27:22 GMT
  Server: Apache
  Location: https://formacionssf.didacsis.com/
  Content-Length: 242
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html; charset=iso-8859-1

Response Body :

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
```

```
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://formacionssf.didacsis.com/">here</a>.</p>
</body></html>
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: New

```
Response Code : HTTP/1.1 401 Unauthorized

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Wed, 09 Nov 2022 13:27:31 GMT
  Server: cPanel
  Persistent-Auth: false
  Host: formacionssf.didacsis.com:2091
  Connection: close
  WWW-Authenticate: Basic realm="Restricted Area"
  Content-Length: 35
  Content-Type: text/html; charset="utf-8"

Response Body :

<html>Authorization Required</html>
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: New

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Date: Wed, 09 Nov 2022 13:27:23 GMT
  Server: Apache
  Content-Language: es-co
  Content-Script-Type: text/javascript
  Content-Style-Type: text/css
  X-UA-Compatible: IE=edge
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-transform
  Pragma: no-cache
  Expires: Mon, 20 Aug 1969 09:23:00 GMT
  Accept-Ranges: none
  X-Frame-Options: sameorigin
  Set-Cookie: MoodleSession=256824d6f53b9a5ee2c4b4638ba38f5a; path=/moodle/; secure
  Upgrade: h2,h2c
  Connection: Upgrade, close
  Last-Modified: Wed, 09 Nov 2022 13:27:23 GMT
  content-Security-Policy: upgrade-insecure-requests
  Transfer-Encoding: chunked
  Content-Type: text/html; charset=utf-8

Response Body :

<!DOCTYPE html>

    <html  dir="ltr" lang="es-co" xml:lang="es-co">
    <head>
        <title>Superintendencia de Subsidio Familiar</title>
        <link rel="shortcut icon" href="https://formacionssf.didacsis.com/moodle/theme/image.php/
_s/moove/theme/1664460099/favicon" />
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="keywords" content="moodle, Superintendencia de Subsidio Familiar" />
<link rel="stylesheet" type="text/css" href="https://formacionssf.didacsis.com/moodle/theme/
yui_combo.php?rollup/3.17.2/yui-moodlesimple-min.css" /><script id="firstthemesheet" type="text/
css">/** Required in order to fix style inclusion problems in IE with YUI **/</script><link
 rel="stylesheet" type="text/css" href="https://formacionssf.didacsis.com/moodle/theme/styles.php/
_s/moove/1664460099_1/all/chunk0" />
```

```
<script>
//<![CDATA[
var M = {}; M.yui = {};
M.pageloadstarttime = new Date();
M.cfg = [...]
```

54582 - SMTP Service Cleartext Login Permitted

Synopsis

The remote mail server allows cleartext logins.

Description

The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Configure the service to support less secure authentication mechanisms only over an encrypted channel.

Risk Factor

Low

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/05/19, Modification date: 2021/01/19

Ports

formacionssf.didacsis.com (TCP/25) Vulnerability State: Active

```
The SMTP server advertises the following SASL methods over an
unencrypted channel on port 25 :

  All supported methods : LOGIN, PLAIN
  Cleartext methods     : LOGIN, PLAIN
```

formacionssf.didacsis.com (TCP/587) Vulnerability State: Active

```
The SMTP server advertises the following SASL methods over an
unencrypted channel on port 587 :

  All supported methods : LOGIN, PLAIN
  Cleartext methods     : LOGIN, PLAIN
```

11414 - IMAP Service Banner Retrieval

Synopsis

An IMAP server is running on the remote host.

Description

An IMAP (Internet Message Access Protocol) server is installed and running on the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2003/03/18, Modification date: 2011/03/16

Ports

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ STARTTLS
 AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: Active

```
The remote imap server banner is :

* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE NAMESPACE LITERAL+ AUTH=PLAIN
 AUTH=LOGIN] Dovecot ready.
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/07/02, Modification date: 2021/05/19

Ports

formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

11111 - RPC Services Enumeration

Synopsis

An ONC RPC service is running on the remote host.

Description

By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2002/08/24, Modification date: 2011/05/24

Ports

formacionssf.didacsis.com (TCP/111) Vulnerability State: New

```
The following RPC services are available on TCP port 111 :

 - program: 100000 (portmapper), version: 4
 - program: 100000 (portmapper), version: 3
 - program: 100000 (portmapper), version: 2
```

formacionssf.didacsis.com (UDP/111) Vulnerability State: New

```
The following RPC services are available on UDP port 111 :

 - program: 100000 (portmapper), version: 4
 - program: 100000 (portmapper), version: 3
 - program: 100000 (portmapper), version: 2
```

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2016/11/14, Modification date: 2018/11/15

Ports

formacionssf.didacsis.com (TCP/2096) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/993) Vulnerability State: New

```
The following root Certification Authority certificate was found :
```

```
|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/110) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/143) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
```

```
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

formacionssf.didacsis.com (TCP/995) Vulnerability State: New

```
The following root Certification Authority certificate was found :

|-Subject             : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Issuer              : C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA
 Certificate Services
|-Valid From          : Jan 01 00:00:00 2004 GMT
|-Valid To            : Dec 31 23:59:59 2028 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS Base Score

6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2017/11/22, Modification date: 2020/03/31

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
TLSv1 is enabled and the server supports at least one cipher.
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time

- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2005/08/26, Modification date: 2022/06/09

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 10.4.1
Nessus build : 20091
Plugin feed version : 202211081550
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : amzn2-aarch64
Scan type : Normal
Scan name : formacionssf.didacsis.com/
Scan policy used : Advanced Network Scan
Scanner IP : tenable.io Scanner
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 123.265 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 800
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Scan Start Date : 2022/11/9 13:06 UTC
Scan duration : 1970 sec
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2487

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/10/09, Modification date: 2019/03/20

Ports

formacionssf.didacsis.com (TCP/25) Vulnerability State: Active

```
The remote SMTP service responded to the 'STARTTLS' command with a
'220' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

formacionssf.didacsis.com (TCP/587) Vulnerability State: Active

```
The remote SMTP service responded to the 'STARTTLS' command with a
'220' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

54580 - SMTP Authentication Methods

Synopsis

The remote mail server supports authentication.

Description

The remote SMTP server advertises that it supports authentication.

See Also

https://tools.ietf.org/html/rfc4422

https://tools.ietf.org/html/rfc4954

Solution

Review the list of methods and whether they're available over an encrypted channel.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/05/19, Modification date: 2019/03/05

Ports

formacionssf.didacsis.com (TCP/25) Vulnerability State: Active

```
The following authentication methods are advertised by the SMTP
server without encryption :
  LOGIN
  PLAIN
```

formacionssf.didacsis.com (TCP/587) Vulnerability State: Active

```
The following authentication methods are advertised by the SMTP
server without encryption :
  LOGIN
```

```
PLAIN
```

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.
Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

See Also

Solution

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk Factor

None

References

XREF	IAVT:0001-T-0932

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/10/12, Modification date: 2020/09/22

Ports

formacionssf.didacsis.com (TCP/25) Vulnerability State: Active

```
Remote SMTP server banner :

220-6050329.didacsis.com ESMTP Exim 4.95 #2 Wed, 09 Nov 2022 07:07:06 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

formacionssf.didacsis.com (TCP/587) Vulnerability State: Active

```
Remote SMTP server banner :

220-6050329.didacsis.com ESMTP Exim 4.95 #2 Wed, 09 Nov 2022 07:06:46 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
Remote SMTP server banner :

220-6050329.didacsis.com ESMTP Exim 4.95 #2 Wed, 09 Nov 2022 07:08:02 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2020/07/09, Modification date: 2020/07/09

Ports

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2019/01/08, Modification date: 2020/08/07

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/05/23, Modification date: 2022/09/09

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

```
Remote device type : general-purpose
Confidence level : 59
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :
```

```
  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for [...]
```

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

Risk Factor

Low

Vulnerability Priority Rating (VPR)

4.4

CVSS v3.0 Base Score

5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CVSS v3.0 Temporal Score

5.2 (E:U/RL:O/RC:C)

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score

1.9 (E:U/RL:OF/RC:C)

References

CVE	CVE-2007-1858
BID	28482

Exploitable with

MetasploitCANVASCore Impact

Plugin Information:

Publication date: 2008/03/28, Modification date: 2021/02/03

Ports

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption
MAC
    ----------------------        ----------       ---           ----     ---------------------
---
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
MAC
    ----------------------        ----------       ---           ----     ---------------------
---
    AECDH-AES128-SHA              0xC0, 0x18       ECDH          None     AES-CBC(128)
SHA1
    AECDH-AES256-SHA              0xC0, 0x19       ECDH          None     AES-CBC(256)
SHA1
    AECDH-RC4-SHA                 0xC0, 0x16       ECDH          None     RC4(128)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
The following is a list of SSL anonymous ciphers supported by the remote TCP server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption
MAC
    ----------------------        ----------       ---           ----     ---------------------
---
    AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH          None     3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)
```

```
   Name                          Code            KEX          Auth     Encryption
MAC
   ----------------------        ----------      ---          ----     --------------------
---
   AECDH-AES128-SHA              0xC0, 0x18      ECDH         None     AES-CBC(128)
SHA1
   AECDH-AES256-SHA              0xC0, 0x19      ECDH         None     AES-CBC(256)
SHA1
   AECDH-RC4-SHA                 0xC0, 0x16      ECDH         None     RC4(128)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

53335 - RPC portmapper (TCP)

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.
The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/04/08, Modification date: 2011/08/29

Ports

formacionssf.didacsis.com (TCP/111) Vulnerability State: New

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2002/03/06, Modification date: 2021/01/19

Ports

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

10185 - POP Server Detection

Synopsis

A POP server is listening on the remote port.

Description

The remote host is running a server that understands the Post Office Protocol (POP), used by email clients to retrieve messages from a server, possibly across a network link.

See Also

https://en.wikipedia.org/wiki/Post_Office_Protocol

Solution

Disable this service if you do not use it.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/10/12, Modification date: 2019/11/22

Ports

formacionssf.didacsis.com (TCP/995) Vulnerability State: Active

```
Remote POP server banner :

+OK Dovecot ready.
```

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

```
Remote POP server banner :

+OK Dovecot ready.
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports
formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
Give Nessus credentials to perform local checks.
```

42149 - FTP Service AUTH TLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote FTP service supports the use of the 'AUTH TLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc4217

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/10/15, Modification date: 2022/02/11

Ports
formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
The remote FTP service responded to the 'AUTH TLS' command with a
'234' response code, suggesting that it supports that command.  However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/~bodo/tls-cbc.txt

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/10/22, Modification date: 2021/02/03

Ports

formacionssf.didacsis.com (TCP/465) Vulnerability State: Active

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    EDH-RSA-DES-CBC3-SHA          0x00, 0x16        DH            RSA       3DES-CBC(168)
SHA1
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA       3DES-CBC(168)
SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17        ECDH          None      3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA       3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    DHE-RSA-AES128-SHA            0x00, 0x33        DH            RSA       AES-CBC(128)
SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39        DH            RSA       AES-CBC(256)
SHA1
    DHE-RSA-CAMELLIA128-SHA       0x00, 0x45        DH            RSA       Camellia-CBC(128)
SHA1
    DHE-RSA-CAMELLIA256-SHA       0x00, 0x88        DH            RSA       Camellia-CBC(256)
SHA1
    DHE-RSA-SEED-SHA              0x00, 0x9A        DH            RSA       SEED-CBC(128)
SHA1
    ECDHE-RSA-AES128-SHA          0xC0, 0x13        ECDH          RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14        ECDH          RSA       AES-CBC(256)
SHA1
    AECDH-AES128-SHA              0xC0, 0x18        ECDH          None      AES-CBC(128)
SHA1
    AECDH-AES256-SHA              0xC0, 0x19        ECDH          None      AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F        RSA           RSA       AES-CBC(128)
SHA1
    AES256-SHA                    [...]
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
    ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12        ECDH          RSA       3DES-CBC(168)
SHA1
    AECDH-DES-CBC3-SHA            0xC0, 0x17        ECDH          None      3DES-CBC(168)
SHA1
    DES-CBC3-SHA                  0x00, 0x0A        RSA           RSA       3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth      Encryption
MAC
    ----------------------        ----------        ---           ----      --------------------
---
```

```
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   AECDH-AES128-SHA              0xC0, 0x18       ECDH          None     AES-CBC(128)
SHA1
   AECDH-AES256-SHA              0xC0, 0x19       ECDH          None     AES-CBC(256)
SHA1
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   IDEA-CBC-SHA                  0x00, 0x07       RSA           RSA      IDEA-CBC(128)
SHA1
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
SHA1
   ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
SHA256
   ECDHE-RSA-AES256-SHA384       [...]
```

formacionssf.didacsis.com (TCP/389) Vulnerability State: Active

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX           Auth     Encryption
MAC
   ----------------------        ----------       ---           ----     ---------------------
---
   AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA               0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA               0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   IDEA-CBC-SHA                  0x00, 0x07       RSA           RSA      IDEA-CBC(128)
SHA1
   SEED-SHA                      0x00, 0x96       RSA           RSA      SEED-CBC(128)
SHA1
   RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.
Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.
Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2013/09/03, Modification date: 2018/11/15

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : CN=6050329.didacsis.com
|-RSA Key Length : 1024 bits
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/05/16, Modification date: 2019/03/06

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

11424 - WebDAV Detection

Synopsis

The remote server is running with WebDAV enabled.

Description

WebDAV is an industry standard extension to the HTTP specification.
It adds a capability for authorized users to remotely add and manage the content of a web server.

If you do not use this extension, you should disable it.

See Also

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2003/03/20, Modification date: 2011/03/14

Ports

formacionssf.didacsis.com (TCP/2078) Vulnerability State: New

34043 - PowerDNS Version Detection

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running PowerDNS, an open source DNS server. It was possible to extract the version number of the remote installation by sending a special DNS request for the text 'version.pdns' in the domain 'chaos'.

See Also

Solution

If desired, hide the version number of PowerDNS by modifying the 'version-string' option in pdns.conf or recursor.conf.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2008/08/25, Modification date: 2019/11/22

Ports

formacionssf.didacsis.com (UDP/53) Vulnerability State: Active

```
  Query method   : version.pdns
  Version source : PowerDNS Authoritative Server 4.4.1 (built May 12 2022 16:30:11 by root@bh-
centos-7.dev.cpanel.net)
  Version        : 4.4.1
  Type           : Authoritative Server
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/04/21, Modification date: 2022/10/05

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
  cpe:/a:mysql:mysql -> MySQL MySQL
  cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

See Also

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2012/01/17, Modification date: 2022/06/14

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=6050329.didacsis.com
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:
TLSv1.3:
- 0x13,0x01 TLS_AES_128_GCM_SHA256
- 0x13,0x02 TLS_AES_256_GCM_SHA384
- 0x13,0x03 TLS_CHACHA20_POLY1305_SHA256
TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
- 0x00,0x9E DHE-RSA-AES128-GCM-SHA256
- 0x00,0x9F DHE-RSA-AES256-GCM-SHA384
This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/01/20, Modification date: 2022/04/06

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites
outlined below:


 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                         Code             KEX           Auth     Encryption
MAC
   ---------------------        ----------       ---           ----     --------------------
---
   DES-CBC3-SHA                 0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

 High Strength Ciphers (>= 112-bit key)

   Name                         Code             KEX           Auth     Encryption
MAC
   ---------------------        ----------       ---           ----     --------------------
---
   RSA-AES128-SHA256            0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384            0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   AES128-SHA                   0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                   0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA              0x00, 0x41       RSA           RSA      Camellia-CBC(128)
SHA1
   CAMELLIA256-SHA              0x00, 0x84       RSA           RSA      Camellia-CBC(256)
SHA1
   IDEA-CBC-SHA                 0x00, 0x07       RSA           RSA      IDEA-CBC(128)
SHA1
```

```
   RC4-MD5                      0x00, 0x04       RSA           RSA      RC4(128)
MD5
   RC4-SHA                      0x00, 0x05       RSA           RSA      RC4(128)
SHA1
   SEED-SHA                     0x00, 0x96       RSA           RSA      SEED-CBC(128)
SHA1
   RSA-AES128-SHA256            0x00, 0x3C       RSA           RSA      AES-CBC(128)
SHA256
   RSA-AES256-SHA256            0x00, 0x3D       RSA           RSA      AES-CBC(256)
SHA256

The fields above are :

 {Tenable ciphername}
 {Cipher ID code}
 Kex={key exchange}
 [...]
```

formacionssf.didacsis.com (TCP/21) Vulnerability State: New

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites
outlined below:


 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                         Code             KEX           Auth     Encryption
MAC
   ---------------------        ----------       ---           ----     --------------------
---
   ECDHE-RSA-DES-CBC3-SHA       0xC0, 0x12       ECDH          RSA      3DES-CBC(168)
SHA1
   AECDH-DES-CBC3-SHA           0xC0, 0x17       ECDH          None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                 0x00, 0x0A       RSA           RSA      3DES-CBC(168)
SHA1

 High Strength Ciphers (>= 112-bit key)

   Name                         Code             KEX           Auth     Encryption
MAC
   ---------------------        ----------       ---           ----     --------------------
---
   RSA-AES128-SHA256            0x00, 0x9C       RSA           RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384            0x00, 0x9D       RSA           RSA      AES-GCM(256)
SHA384
   ECDHE-RSA-AES128-SHA         0xC0, 0x13       ECDH          RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA         0xC0, 0x14       ECDH          RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-RC4-SHA            0xC0, 0x11       ECDH          RSA      RC4(128)
SHA1
   AECDH-AES128-SHA             0xC0, 0x18       ECDH          None     AES-CBC(128)
SHA1
   AECDH-AES256-SHA             0xC0, 0x19       ECDH          None     AES-CBC(256)
SHA1
   AECDH-RC4-SHA                0xC0, 0x16       ECDH          None     RC4(128)
SHA1
   AES128-SHA                   0x00, 0x2F       RSA           RSA      AES-CBC(128)
SHA1
   AES256-SHA                   0x00, 0x35       RSA           RSA      AES-CBC(256)
SHA1
   CAMELLIA128-SHA              0x00, 0x41       RSA           RSA      Camellia-CBC(128)
[...]
```

formacionssf.didacsis.com (TCP/465) Vulnerability State: New

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites
outlined below:


 Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                         Code             KEX           Auth     Encryption
MAC
```

```
   ----------------------        ----------       ---          ----     --------------------
---
   EDH-RSA-DES-CBC3-SHA          0x00, 0x16       DH           RSA      3DES-CBC(168)
SHA1
   ECDHE-RSA-DES-CBC3-SHA        0xC0, 0x12       ECDH         RSA      3DES-CBC(168)
SHA1
   AECDH-DES-CBC3-SHA            0xC0, 0x17       ECDH         None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                  0x00, 0x0A       RSA          RSA      3DES-CBC(168)
SHA1

 High Strength Ciphers (>= 112-bit key)

   Name                          Code             KEX          Auth     Encryption
MAC
   ----------------------        ----------       ---          ----     --------------------
---
   RSA-AES128-SHA256             0x00, 0x9C       RSA          RSA      AES-GCM(128)
SHA256
   RSA-AES256-SHA384             0x00, 0x9D       RSA          RSA      AES-GCM(256)
SHA384
   DHE-RSA-AES128-SHA            0x00, 0x33       DH           RSA      AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA            0x00, 0x39       DH           RSA      AES-CBC(256)
SHA1
   DHE-RSA-CAMELLIA128-SHA       0x00, 0x45       DH           RSA      Camellia-CBC(128)
SHA1
   DHE-RSA-CAMELLIA256-SHA       0x00, 0x88       DH           RSA      Camellia-CBC(256)
SHA1
   DHE-RSA-SEED-SHA              0x00, 0x9A       DH           RSA      SEED-CBC(128)
SHA1
   ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH         RSA      AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH         RSA      AES-CBC(256)
SHA1
   ECDHE-RSA-RC4-SHA             0xC0, 0x11       ECDH         RSA      RC4(128)
[...]
```

157288 - TLS Version 1.1 Protocol Deprecated

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

http://www.nessus.org/u?c8ae820d

https://datatracker.ietf.org/doc/html/rfc8996

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSS Base Score

6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2022/04/04, Modification date: 2022/04/11

Ports
formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/orig.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/10/12, Modification date: 2018/11/15

Ports
formacionssf.didacsis.com (TCP/2096) Vulnerability State: Active

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

formacionssf.didacsis.com (TCP/2087) Vulnerability State: Active

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

formacionssf.didacsis.com (TCP/2083) Vulnerability State: Active

```
Contents of robots.txt :

User-agent: *
Disallow: /
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

See Also

Solution

N/A

Risk Factor

None

References

XREF IAVT:0001-T-0931

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2000/01/04, Modification date: 2020/10/30

Ports

formacionssf.didacsis.com (TCP/80) Vulnerability State: Active

```
The remote web server type is :

Apache
```

formacionssf.didacsis.com (TCP/2078) Vulnerability State: Active

```
The remote web server type is :

cPanel
```

formacionssf.didacsis.com (TCP/2091) Vulnerability State: Active

```
The remote web server type is :

cPanel
```

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
The remote web server type is :

Apache
```

formacionssf.didacsis.com (TCP/2080) Vulnerability State: Active

```
The remote web server type is :

cPanel
```

11002 - DNS Server Detection

Synopsis

A DNS server is listening on the remote host.

Description

The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

See Also

https://en.wikipedia.org/wiki/Domain_Name_System

Solution

Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2003/02/13, Modification date: 2017/05/16

Ports

formacionssf.didacsis.com (TCP/53) Vulnerability State: Active

formacionssf.didacsis.com (UDP/53) Vulnerability State: Active

42087 - POP3 Service STLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote POP3 service supports the use of the 'STLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://tools.ietf.org/html/rfc2595

https://en.wikipedia.org/wiki/STARTTLS

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/10/09, Modification date: 2021/02/24

Ports

formacionssf.didacsis.com (TCP/110) Vulnerability State: Active

```
The remote POP3 service responded to the 'STLS' command with an
'+OK' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2011/02/07, Modification date: 2021/09/13

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
This port supports resuming SSLv3 sessions.
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

N/A

Risk Factor

None

References

XREF IAVT:0001-T-0530

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/07/30, Modification date: 2022/09/08

Ports

formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
URL        : https://formacionssf.didacsis.com/
Version    : unknown
Source     : Server: Apache
backported : 0
```

formacionssf.didacsis.com (TCP/80) Vulnerability State: Active

```
URL        : http://formacionssf.didacsis.com/
Version    : unknown
Source     : Server: Apache
backported : 0
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

See Also

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/05/08, Modification date: 2015/05/08

Ports

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=6050329.didacsis.com
|-Not After : Nov 15 23:59:59 2022 GMT
```

42085 - IMAP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

The remote IMAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://tools.ietf.org/html/rfc2595

https://en.wikipedia.org/wiki/STARTTLS

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/10/09, Modification date: 2021/02/24

Ports

formacionssf.didacsis.com (TCP/143) Vulnerability State: Active

```
The remote IMAP service responded to the 'STARTTLS' command with an
'OK' response code, suggesting that it supports that command. However,
Nessus failed to negotiate a TLS connection or get the associated SSL
certificate, perhaps because of a network connectivity problem or the
service requires a peer certificate as part of the negotiation.
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.
There are several possible reasons for this :
- The scan may have caused a service to freeze or stop running.
- An administrator may have stopped a particular service during the scanning process.
This might be an availability problem related to the following :
- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.
- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.
In any case, the audit of the remote host might be incomplete and may need to be done again.

See Also

Solution

- Increase checks_read_timeout and/or reduce max_checks.
- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF	IAVB:0001-B-0509

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2002/03/19, Modification date: 2021/07/23

Ports
formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

```
Port 110 was detected as being open but is now closed
Port 389 was detected as being open but is now closed
Port 143 was detected as being open but is now closed
Port 21 was detected as being open but is now closed
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/07/17, Modification date: 2021/02/03

Ports
formacionssf.didacsis.com (TCP/443) Vulnerability State: Active

```
http/1.1
h2
```

85805 - HTTP/2 Cleartext Detection

Synopsis

An HTTP/2 server is listening on the remote host.

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2015/09/04, Modification date: 2022/04/11

Ports
formacionssf.didacsis.com (TCP/80) Vulnerability State: Active

```
The server supports direct HTTP/2 connections
```

```
without encryption.
```

149334 - SSH Password Authentication Accepted

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/05/07, Modification date: 2021/05/07

Ports

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

10223 - RPC portmapper Service Detection

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.
The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.

See Also

Solution

N/A

Risk Factor

None

Vulnerability Priority Rating (VPR)

0.8

CVSS v3.0 Base Score

0.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS Base Score

0.0 (AV:N/AC:L/Au:N/C:N/I:N/A:N)

References

CVE CVE-1999-0632

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/08/19, Modification date: 2019/10/04

Ports

formacionssf.didacsis.com (UDP/111) Vulnerability State: New

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD
Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response.
If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/12/10, Modification date: 2022/04/11

Ports

formacionssf.didacsis.com (TCP/2078) Vulnerability State: New

```
Based on the response to an OPTIONS request :

  - HTTP methods  COPY  DELETE  GET  HEAD  LOCK  MKCOL  MOVE  POST
    PROPFIND  PROPPATCH  PUT  UNLOCK OPTIONS are allowed on :

    /
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2004/02/11, Modification date: 2017/04/14

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

```
162.214.64.97 resolves as 6050329.didacsis.com.
```

25701 - LDAP Crafted Search Request Server Information Disclosure

Synopsis

It is possible to discover information about the remote LDAP server.

Description

By sending a search request with a filter set to 'objectClass=*', it is possible to extract information about the remote LDAP server.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2007/07/12, Modification date: 2022/09/28

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
[+]-namingContexts:
   |  dc=my-domain,dc=com
[+]-objectClass:
   |  top
   |  OpenLDAProotDSE
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.
Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.
Note that this plugin only checks for the options of the remote SSH server.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/09/23, Modification date: 2022/04/05

Ports

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

```
The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/10/12, Modification date: 2019/11/22

Ports

formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
The remote FTP banner is :

220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 08:08. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.
An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

http://www.nessus.org/u?5d15ba70

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS Base Score

10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2005/10/12, Modification date: 2022/04/04

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
- SSLv3 is enabled and the server supports at least one cipher.
 Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption
MAC
    ----------------------        ----------       ---           ----     --------------------
---
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)
SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
MAC
    ----------------------        ----------       ---           ----     --------------------
---
    AES128-SHA                                     RSA           RSA      AES-CBC(128)
SHA1
    AES256-SHA                                     RSA           RSA      AES-CBC(256)
SHA1
    CAMELLIA128-SHA                                RSA           RSA      Camellia-CBC(128)
SHA1
    CAMELLIA256-SHA                                RSA           RSA      Camellia-CBC(256)
SHA1
    IDEA-CBC-SHA                                   RSA           RSA      IDEA-CBC(128)
SHA1
    RC4-MD5                                        RSA           RSA      RC4(128)
MD5
    RC4-SHA                                        RSA           RSA      RC4(128)
SHA1
    SEED-SHA                                       RSA           RSA      SEED-CBC(128)
SHA1
    RSA-AES128-SHA256                              RSA           RSA      AES-CBC(128)
SHA256
    RSA-AES256-SHA256                              RSA           RSA      AES-CBC(256)
SHA256

The fields above are :

  {Tenable ciphername}
```

```
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/12/15, Modification date: 2020/04/27

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=6050329.didacsis.com
|-Issuer  : CN=6050329.didacsis.com
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/11/30, Modification date: 2020/06/12

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

42329 - LDAP Service STARTTLS Command Support

Synopsis

The remote directory service supports encrypting traffic.

Description

The remote LDAP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.

See Also

https://en.wikipedia.org/wiki/STARTTLS

https://tools.ietf.org/html/rfc2830

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/10/30, Modification date: 2021/02/24

Ports

formacionssf.didacsis.com (TCP/389) Vulnerability State: New

```
Here is the LDAP server's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

------------------------------ snip ------------------------------
Subject Name:

Common Name: 6050329.didacsis.com

Issuer Name:

Common Name: 6050329.didacsis.com

Serial Number: 00 BD 17 D4 6F

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption
```

```
Not Valid Before: Sep 15 22:19:27 2022 GMT
Not Valid After: Sep 15 22:19:27 2023 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 BB A9 92 10 5E F9 82 B2 A2 D2 DA 9D 81 21 B0 E4 E8 57 DB
            25 25 F0 5C 65 78 41 E2 73 94 69 35 5C C6 A1 F4 94 E6 F8 34
            D7 9F 31 9F 7E B9 7D 4A 6F A9 62 75 34 C8 90 0E E6 60 9A DF
            54 E6 5D 5E B5 AD 55 85 97 A0 E1 74 8F C2 61 EE 3C 55 EB A8
            10 0F 3E C1 E7 8C A3 A0 0F F8 86 CC F6 F3 14 D2 F3 0D 40 D1
            93 C5 55 D3 98 A6 71 C1 FA B3 EC CA 75 11 0D 88 86 F2 C4 18
            84 23 3E 9C F8 5D A5 C4 3D
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 B1 2C 2E B3 35 80 1C 71 94 62 7A CF 4B E7 EE DE 65 FF B1
           2D D1 A1 55 D0 C8 63 C7 00 C7 B7 BE CA 63 06 B0 5D 33 3A BC
           7F B9 FE 1B A6 24 24 9D AE 2C 62 C2 5E 36 3A B7 AE BE DC 4E
           BD F6 39 99 ED 79 FF DB E6 5A 04 C7 87 4E CF 55 C8 CD 70 A1
           41 B2 18 62 D8 0C 73 2E 40 D4 0A 9D 39 FF E9 9B 7B 17 87 5D
           60 50 34 A1 B5 31 14 8A 91 E2 10 1E 14 3D F4 C8 7B B1 8A 2B
           3A 91 1F DE E3 77 6B 7A 50

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: 6050329.didacsis.com
DNS: localhost
DNS: localhost.localdomain


------------------------------ snip ------------------------------
```

10114 - ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

See Also

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

None

Vulnerability Priority Rating (VPR)

0.0

CVSS v3.0 Base Score

0.0 (AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)

CVSS Base Score

0.0 (AV:L/AC:L/Au:N/C:N/I:N/A:N)

References

CVE	CVE-1999-0524
XREF	CWE:200

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/08/01, Modification date: 2019/10/04

Ports

formacionssf.didacsis.com (ICMP/0) Vulnerability State: New

```
The remote clock is synchronized with the local clock.
```

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

See Also

Solution

N/A

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/10/12, Modification date: 2020/09/22

Ports

formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
SSH version : SSH-2.0-OpenSSH_7.4
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic,password
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

See Also

Solution

N/A

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 1999/11/27, Modification date: 2020/08/20

Ports

formacionssf.didacsis.com (UDP/0) Vulnerability State: Active

```
For your information, here is the traceroute from 172.16.2.166 to 162.214.64.97 :
172.16.2.166
3.236.60.161
241.0.11.209
```

```
240.0.160.24
242.2.11.17
52.93.29.41
100.100.2.106
128.241.4.57
129.250.2.124
129.250.3.189
129.250.3.142
168.143.228.173
162.215.195.128
162.215.195.141
69.195.64.105
162.144.240.17
162.214.64.97

Hop Count: 16
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.
Different web servers may be hosted on name-based virtual hosts.

See Also

https://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
www.example.com[192.0.32.10]

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2010/04/29, Modification date: 2022/08/15

Ports

formacionssf.didacsis.com (TCP/0) Vulnerability State: Active

```
The following hostnames point to the remote host :
  - 6050329.didacsis.com
  - didacsis.com
  - mail.didacsis.com
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

See Also

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2009/12/02, Modification date: 2020/09/04

Ports
formacionssf.didacsis.com (TCP/21) Vulnerability State: Active

```
The SSL certificate will expire within 60 days, at
Nov 15 23:59:59 2022 GMT :

  Subject          : CN=6050329.didacsis.com
  Issuer           : C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification
 Authority
  Not valid before : Aug 17 00:00:00 2022 GMT
  Not valid after  : Nov 15 23:59:59 2022 GMT
```

153953 - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.
This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:
diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
gss-gex-sha1-*
gss-group1-sha1-*
gss-group14-sha1-*
rsa1024-sha1
Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

http://www.nessus.org/u?b02d91cd

https://datatracker.ietf.org/doc/html/rfc8732

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)

Exploitable with

Core ImpactMetasploitCANVAS

Plugin Information:

Publication date: 2021/10/13, Modification date: 2021/10/13

Ports
formacionssf.didacsis.com (TCP/22) Vulnerability State: Active

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

Assets Summary (Executive)

formacionssf.didacsis.com

Summary

Critical	High	Medium	Low	Info	Total
1	1	6	4	63	75

Details

Severity	Plugin Id	Name
Critical	20007	SSL Version 2 and 3 Protocol Detection
High	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
Medium	31705	SSL Anonymous Cipher Suites Supported
Medium	104743	TLS Version 1.0 Protocol Detection
Medium	57582	SSL Self-Signed Certificate
Medium	157288	TLS Version 1.1 Protocol Deprecated
Medium	51192	SSL Certificate Cannot Be Trusted
Medium	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low	70658	SSH Server CBC Mode Ciphers Enabled
Low	153953	SSH Weak Key Exchange Algorithms Enabled
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Low	54582	SMTP Service Cleartext Login Permitted
Info	149334	SSH Password Authentication Accepted
Info	45590	Common Platform Enumeration (CPE)
Info	70657	SSH Algorithms and Languages Supported
Info	11219	Nessus SYN scanner
Info	84502	HSTS Missing From HTTPS Server
Info	72779	DNS Server Version Detection
Info	10107	HTTP Server Type and Version
Info	11424	WebDAV Detection
Info	85805	HTTP/2 Cleartext Detection
Info	136318	TLS Version 1.2 Protocol Detection
Info	42087	POP3 Service STLS Command Support
Info	39520	Backported Security Patch Detection (SSH)
Info	22964	Service Detection
Info	166602	Asset Attribute: Fully Qualified Domain Name (FQDN)

Info	42981	SSL Certificate Expiry - Future Expiry
Info	21643	SSL Cipher Suites Supported
Info	42149	FTP Service AUTH TLS Command Support
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	42085	IMAP Service STARTTLS Command Support
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10263	SMTP Server Detection
Info	10863	SSL Certificate Information
Info	48204	Apache HTTP Server Version
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	43111	HTTP Methods Allowed (per directory)
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	121010	TLS Version 1.1 Protocol Detection
Info	10881	SSH Protocol Versions Supported
Info	100669	Web Application Cookies Are Expired
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	51891	SSL Session Resume Supported
Info	11002	DNS Server Detection
Info	156899	SSL/TLS Recommended Cipher Suites
Info	56984	SSL / TLS Versions Supported
Info	54615	Device Type
Info	11111	RPC Services Enumeration
Info	11414	IMAP Service Banner Retrieval
Info	53335	RPC portmapper (TCP)
Info	25220	TCP/IP Timestamps Supported
Info	84821	TLS ALPN Supported Protocol Enumeration
Info	11936	OS Identification
Info	10386	Web Server No 404 Error Code Check
Info	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
Info	10287	Traceroute Information

Info	50845	OpenSSL Detection
Info	10267	SSH Server Type and Version Information
Info	34043	PowerDNS Version Detection
Info	46180	Additional DNS Hostnames
Info	42329	LDAP Service STARTTLS Command Support
Info	94761	SSL Root Certification Authority Certificate Information
Info	19506	Nessus Scan Information
Info	10919	Open Port Re-check
Info	10302	Web Server robots.txt Information Disclosure
Info	138330	TLS Version 1.3 Protocol Detection
Info	153588	SSH SHA-1 HMAC Algorithms Enabled
Info	54580	SMTP Authentication Methods
Info	10092	FTP Server Detection
Info	10185	POP Server Detection
Info	42088	SMTP Service STARTTLS Command Support
Info	10223	RPC portmapper Service Detection
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	20870	LDAP Server Detection