Domain controller - Not updated

Report generated by Nessus™ Thu, 27 Aug 2020 15:01:47 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.43.21

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	33

Scan Information

Start time: Thu Aug 27 14:55:41 2020
End time: Thu Aug 27 15:01:46 2020

Host Information

IP: 192.168.43.21
MAC Address: 00:0C:29:E0:B2:21
OS: Linux Kernel 5.7.0-kali1-amd64

Vulnerabilities

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 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/8834/www

```
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 : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=linux
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

12634 - Authenticated Check : OS Name and Installed Package Enumeration

Synopsis

This plugin gathers information about the remote host via an authenticated session.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet, or local commands and extracts the list of installed packages.

If using SSH, the scan should be configured with a valid SSH public key and possibly an SSH passphrase (if the SSH public key is protected by a passphrase).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/07/06, Modified: 2020/07/23

Plugin Output

tcp/0

```
Nessus can run commands on localhost to check if patches are applied.

The output of "uname -a" is :
Linux linux 5.7.0-kali1-amd64 #1 SMP Debian 5.7.6-1kali2 (2020-07-01) x86_64 GNU/Linux

Local security checks have NOT been enabled because the remote Linux
distribution is not supported.
```

110695 - Authentication Success - Local Checks Not Available

Synopsis

The local security checks are unavailable.

Description

Local security checks are not available for this host because they may be infeasible or may not be supported by Nessus. The credentials supplied in the scan policy may have been successful, but local security checks cannot be performed at this time.

Solution

If local security checks are required for this host, contact Tenable support.

Risk Factor

None

References

XREF IAVB:0001-B-521

Plugin Information

Published: 2018/06/26, Modified: 2020/08/25

Plugin Output

tcp/0

```
A successful connection to the remote host was established, but local
security checks are not available.

Plugin      : ssh_get_info.nasl
Plugin ID   : 12634
Plugin Name : Authenticated Check : OS Name and Installed Package Enumeration
Report      :
====================
Nessus can run commands on localhost to check if patches are applied.

The output of "uname -a" is :
Linux linux 5.7.0-kali1-amd64 #1 SMP Debian 5.7.6-1kali2 (2020-07-01) x86_64 GNU/Linux

Local security checks have NOT been enabled because the remote Linux
distribution is not supported.
====================
```

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

Plugin Information

Published: 2010/04/21, Modified: 2020/08/20

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel:5.7

Following application CPE matched on the remote system :

  cpe:/a:tenable:nessus:18.11.1
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

This plugin reports a device's hostname collected via SSH or WMI.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2020/08/20

Plugin Output

tcp/0

```
Hostname : linux
  linux (hostname command)
```

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).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2017/01/26

Plugin Output

tcp/0

```
The following IPv4 addresses are set on the remote host :

 - 192.168.43.21 (on interface eth0)
 - 127.0.0.1 (on interface lo)
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

Nessus was able to enumerate the IPv6 interfaces on the remote host.

Description

Nessus was able to enumerate the network interfaces configured with IPv6 addresses by connecting to the remote host via SSH using the supplied credentials.

Solution

Disable IPv6 if you are not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2017/01/26

Plugin Output

tcp/0

```
The following IPv6 interfaces are set on the remote host :

 - 2402:8100:2219:fdae:20c:29ff:fee0:b221 (on interface eth0)
 - 2402:8100:2219:fdae:350e:e39b:8453:2adc (on interface eth0)
 - fe80::20c:29ff:fee0:b221 (on interface eth0)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

Nessus was able to enumerate MAC addresses on the remote host.

Description

Nessus was able to enumerate MAC addresses by connecting to the remote host via SSH with the supplied credentials.

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following MAC address exists on the remote host :

  - 00:0c:29:e0:b2:21 (interface eth0)
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:0C:29:E0:B2:21 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:0C:29:E0:B2:21
```

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.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-931

Plugin Information

Published: 2000/01/04, Modified: 2020/08/25

Plugin Output

tcp/8834/www

```
The remote web server type is :

NessusWWW
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.43.21 resolves as linux.
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/8834/www

```
Response Code : HTTP/1.1 200 OK

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

  Cache-Control: must-revalidate
  X-Frame-Options: DENY
  Content-Type: text/html
  ETag: ee3b5fcbfc545ad7e1b58ed1fb4e61de
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Thu, 27 Aug 2020 18:55:55 GMT
  X-Content-Type-Options: nosniff
  Content-Length: 861
  Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action 'self';
 frame-ancestors 'none'; frame-src https://store.tenable.com; default-src 'self'; script-src 'self';
 img-src 'self' data:; style-src 'self' 'unsafe-inline'; object-src 'none'
  Strict-Transport-Security: max-age=31536000
  Expect-CT: max-age=0

Response Body :

<!doctype html>
```

```
<html lang="en">
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
        <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com; default-src 'self'; script-
src 'self'; img-src 'self' data:; style-src 'self' 'unsafe-inline'; object-src 'none'" />
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <meta charset="utf-8" />
        <title>Nessus</title>
        <link rel="stylesheet" href="nessus6.css?v=1596667901883" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1596667901883"></script>
    </head>
    <body>
    </body>
</html>
```

117886 - Local Checks Not Enabled (info)

Synopsis

Local checks were not enabled.

Description

Nessus did not enable local checks on the remote host. This does not necessarily indicate a problem with the scan. Credentials may not have been provided, local checks may not be available for the target, the target may not have been identified, or another issue may have occurred that prevented local checks from being enabled. See plugin output for details.

This plugin reports informational findings related to local checks not being enabled. For failure information, see plugin 21745 :

'Authentication Failure - Local Checks Not Run'.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-515

Plugin Information

Published: 2018/10/02, Modified: 2020/08/25

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : ssh_get_info2.nasl
    Plugin ID   : 97993
    Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH
 Library)
    Protocol    : LOCALHOST
    Message     : Debian version does not match known patterns

  - Plugin      : hostlevel_checks_unavailable.nasl
    Plugin ID   : 110695
    Plugin Name : Authentication Success - Local Checks Not Available
    Message     : Local security checks are unavailable.
```

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.
- 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2020/08/24

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.11.1
Plugin feed version : 202008271200
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.43.21
Thorough tests : no
Experimental tests : 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 : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/8/27 14:55 EDT
Scan duration : 364 sec
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

https://www.tenable.com/products/nessus/nessus-professional

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF IAVT:0001-T-673

Plugin Information

Published: 1999/10/12, Modified: 2020/08/25

Plugin Output

tcp/8834/www

```
URL              : https://linux:8834/
Version          : 18.11.1
Nessus UI Version : 8.11.1
```

58651 - Netstat Active Connections

Synopsis

Active connections are enumerated via the 'netstat' command.

Description

This plugin runs 'netstat' on the remote machine to enumerate all active 'ESTABLISHED' or 'LISTENING' tcp/udp connections.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/04/10, Modified: 2018/06/19

Plugin Output

tcp/0

```
Netstat output :
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8834            0.0.0.0:*               LISTEN
tcp6       0      0 :::8834                 :::*                    LISTEN
tcp6       0      0 2402:8100:2219:fd:38444 2402:3a80:c00d:23:::443 ESTABLISHED
udp        0      0 192.168.43.21:68        192.168.43.1:67         ESTABLISHED
raw6       0      0 :::58                   :::*                    7
```

64582 - Netstat Connection Information

Synopsis

Nessus was able to parse the results of the 'netstat' command on the remote host.

Description

The remote host has listening ports or established connections that Nessus was able to extract from the results of the 'netstat' command.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2018/05/16

Plugin Output

tcp/0

```
tcp4 (listen)
  src: [host=0.0.0.0, port=8834]
  dst: [host=0.0.0.0, port=*]

tcp6 (listen)
  src: [host=::, port=8834]
  dst: [host=::, port=*]

tcp6 (established)
  src: [host=2402:8100:2219:fd, port=38444]
  dst: [host=2402:3a80:c00d:23::, port=443]

udp4 (established)
  src: [host=192.168.43.21, port=68]
  dst: [host=192.168.43.1, port=67]

udp6 (listen)
  src: [host=::, port=58]
  dst: [host=::, port=*]
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2020/06/12

Plugin Output

tcp/8834/www

```
Port 8834/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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2020/03/09

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 5.7.0-kali1-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 5.7.0-kali1-amd64
```

97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)

Synopsis

Information about the remote host can be disclosed via an authenticated session.

Description

Nessus was able to login to the remote host using SSH or local commands and extract the list of installed packages.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2020/06/12

Plugin Output

tcp/0

```
Nessus can run commands on localhost to check if patches are applied.

The output of "uname -a" is :
Linux linux 5.7.0-kali1-amd64 #1 SMP Debian 5.7.6-1kali2 (2020-07-01) x86_64 GNU/Linux

We are able to run commands on the remote host, but are unable to
currently identify it in this plugin.

Runtime : 1.18788 seconds
```

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

Although this host was scanned through a private IPv4 or local scope IPv6 address, some network interfaces are configured with global scope IPv6 addresses. Depending on the configuration of the firewalls and routers, this host may be reachable from Internet.

Solution

Disable IPv6 if you do not actually using it.

Otherwise, disable any unused IPv6 interfaces and implement IP filtering if needed.

Risk Factor

None

Plugin Information

Published: 2010/04/02, Modified: 2012/08/07

Plugin Output

tcp/0

```
The following global addresss were gathered :

  - 2402:8100:2219:fdae:20c:29ff:fee0:b221
  - 2402:8100:2219:fdae:350e:e39b:8453:2adc
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2020/07/09

Plugin Output

tcp/8834/www

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

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2020/06/17

Plugin Output

tcp/8834/www

```
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: linux

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 77 53

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Aug 27 18:11:20 2020 GMT
Not Valid After: Aug 26 18:11:20 2024 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 CF 51 09 E9 40 52 BC 03 93 B3 98 E4 E6 F8 B1 79 6D 38 59
```

```
             0C 29 21 71 7B 8F E2 FE 62 17 F0 91 DF 4D F3 15 7D 0B 9F C4
             B4 85 94 E1 19 FE 5B 71 16 98 93 36 1D 10 12 E6 CD 49 D9 1D
             10 C2 3B 7F EC FB E0 15 7A 7B 5D F1 CF 14 DF 11 3A 1E 9F 56
             DA 2C E2 FC A6 0C F0 68 F9 02 B3 B8 D5 E0 0C 01 6A 74 B6 D6
             45 3A 3C A7 15 0C AA 50 88 9B 54 43 1D 8C 15 50 94 B4 9A 9F
             DC FA 4C 3C 61 09 38 0A AC 7C C8 BE 5A DE 83 9E 80 1B E5 4D
             F9 94 B7 16 6B A6 41 F9 CF 3D 0E F0 87 62 2A 41 AC BD E9 CF
             2D 7E 98 3A 99 49 51 86 23 EC 45 BA AB 3E AA A8 C5 34 EB E2
             15 85 3F 86 29 4B 47 3C B8 8A 67 24 5B 96 47 F2 80 56 07 E2
             2C 39 D0 F6 50 D7 B9 A3 B9 9E 2C 6E F5 AE 82 9F 1C 2B 93 BB
             3A 91 E1 5E CD 47 FC B8 1A FF 46 62 13 E4 1D 95 6C 5B 93 8C
             9F 31 0A 3A CD A7 A1 E7 7B 05 3A 78 98 C8 34 B5 99
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 15 5C A0 93 C5 7A 48 BB D6 3C 53 A7 EE 46 6A D6 3B A4 AA
           B3 45 66 38 17 C8 94 F9 B9 ED A9 01 80 E8 3A AC E7 CA C6 39
           D6 A3 46 0D CF C4 A9 64 AB 51 E8 E6 B0 AF EB 43 FA 55 FF E4
           0F 3E E7 F0 F6 E9 04 C7 5C 89 BB 54 7C 6A 2E 06 BC 8B 3B 8A
           74 16 E4 46 84 B2 32 AC 78 84 29 03 77 98 2B 73 0F D3 26 AC
           73 4F 4B 5C 91 35 0E 1A C5 63 60 E2 3C 70 21 0A C3 7B 8C E6
           B1 36 5A 6C 0A 44 97 [...]
```

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/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2018/11/15

Plugin Output

tcp/8834/www

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

  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
    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}
```

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/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2020/07/09

Plugin Output

tcp/8834/www

```
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
    ----------------------        ----------       ---           ----     --------------------   ---
    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-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}
```

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

Plugin Information

Published: 2011/12/07, Modified: 2018/11/15

Plugin Output

tcp/8834/www

```
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
    ----------------------       ----------       ---          ----     ---------------------  ---
    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-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}
```

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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2020/08/18

Plugin Output

tcp/8834/www

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

tcp/8834/www

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

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

See Also

http://www.nessus.org/u?2fb3aca6

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2019/11/22

Plugin Output

tcp/8834/www

```
The STS header line is :

Strict-Transport-Security: max-age=31536000
```

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

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/8834/www

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

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

Plugin Information

Published: 2020/07/09, Modified: 2020/07/09

Plugin Output

tcp/8834/www

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

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/10/12, Modified: 2018/06/19

Plugin Output

tcp/0

```
reboot   system boot  5.7.0-kali1-amd6 Thu Aug 27 11:46   still running
reboot   system boot  5.7.0-kali1-amd6 Thu Aug 27 10:40 - 11:28  (00:48)
reboot   system boot  5.7.0-kali1-amd6 Thu Aug 27 09:05 - 09:23  (00:18)
reboot   system boot  5.7.0-kali1-amd6 Thu Aug 27 08:42 - 09:05  (00:23)
reboot   system boot  5.7.0-kali1-amd6 Thu Aug 27 08:09 - 08:27  (00:18)
reboot   system boot  5.7.0-kali1-amd6 Sun Aug 23 09:26 - 11:39  (02:12)
reboot   system boot  5.7.0-kali1-amd6 Sun Aug 23 03:19 - 03:27  (00:07)
reboot   system boot  5.7.0-kali1-amd6 Sun Aug 23 03:12 - 03:14  (00:01)
reboot   system boot  5.7.0-kali1-amd6 Sun Aug 23 02:48 - 02:55  (00:07)
reboot   system boot  5.7.0-kali1-amd6 Sat Aug 22 12:47 - 13:15  (00:27)
reboot   system boot  5.7.0-kali1-amd6 Sat Aug 22 12:12 - 12:23  (00:10)
reboot   system boot  5.7.0-kali1-amd6 Sat Aug 22 11:05 - 12:11  (01:05)
reboot   system boot  5.7.0-kali1-amd6 Tue Aug 18 08:09 - 08:21  (00:12)
reboot   system boot  5.7.0-kali1-amd6 Tue Aug 18 07:02 - 08:08  (01:06)
reboot   system boot  5.7.0-kali1-amd6 Tue Aug 18 00:25 - 01:20  (00:54)
reboot   system boot  5.7.0-kali1-amd6 Mon Aug 17 15:01 - 15:29  (00:27)
reboot   system boot  5.5.0-kali2-amd6 Mon Aug 17 12:24 - 14:53  (02:28)
reboot   system boot  5.5.0-kali2-amd6 Mon Aug 17 11:19 - 12:23  (01:03)
reboot   system boot  5.5.0-kali2-amd6 Sat Aug  1 10:10 - 10:33  (00:23)
reboot   system boot  5.5.0-kali2-amd6 Sat Aug  1 09:31 - 10:04  (00:33)
reboot   system boot  5.5.0-kali2-amd6 Sat Aug  1 05:16 - 05:20  (00:03)
reboot   system boot  5.5.0-kali2-amd6 Sat Aug  1 05:13 - 05:15  (00:02)
reboot   system boot  5.5.0-kali2-amd6 Sat Aug  1 02:49 - 05:13  (02:23)
reboot   system boot  5.5.0-kali2-amd6 Fri Jul 31 16:18 - 16:25  (00:06)

wtmp begins Fri Jul 31 16:18:33 2020
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information

Published: 2005/10/27, Modified: 2019/12/11

Plugin Output

tcp/0

```
The remote host is a VMware virtual machine.
```