# tenable® Nessus

# HAIDEN−HOME−NETWORK−SCAN

# Vulnerabilities by Host

# Vulnerabilities by Host

# 192.168.68.1

| 0 | 0 | 1 | 1 | 36 |
|:---:|:---:|:---:|:---:|:---:|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

## Scan Information

Start time:        Sun Mar 2 19:57:15 2025

End time:        Sun Mar 2 21:02:46 2025

## Host Information

IP:        192.168.68.1

MAC Address:        1C:61:B4:AC:C8:6D

OS:        Linux Kernel 2.2, Linux Kernel 2.4, Linux Kernel 2.6

## 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

## 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 v2.0 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/443/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 : C=CN/CN=tplinkdeco.net
|-Issuer  : C=CN/CN=tplinkdeco.net
```

## 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.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.8939

CVSS v2.0 Base Score

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

References

CVE             CVE-1999-0524
XREF            CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -1 seconds.
```

## 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

### Plugin Information

Published: 2010/04/29, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - tplinkdeco.net
```

## 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: 2025/02/12

Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE matched on the remote system :

  cpe:/a:tp-link:tp-link -> tp-link
```

## 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

### Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

### Plugin Output

tcp/53/dns

## 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

Plugin Information

Published: 2003/02/13, Modified: 2017/05/16

Plugin Output

udp/53/dns

## 132634 - Deprecated SSLv2 Connection Attempts

Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

Plugin Output

tcp/0

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 83742
Timestamp: 2025-03-03 01:01:42
Port: 443

Plugin ID: 159893
Timestamp: 2025-03-03 01:02:15
Port: 443

Plugin ID: 69370
Timestamp: 2025-03-03 01:02:01
Port: 443

Plugin ID: 19590
Timestamp: 2025-03-03 01:01:43
Port: 443

Plugin ID: 14191
Timestamp: 2025-03-03 01:02:16
Port: 443

Plugin ID: 17297
Timestamp: 2025-03-03 01:02:38
Port: 443

Plugin ID: 173741
```

```
Timestamp: 2025-03-03 01:02:18
Port: 443

Plugin ID: 84216
Timestamp: 2025-03-03 01:02:38
Port: 443

Plugin ID: 184237
Timestamp: 2025-03-03 01:02:18
Port: 443

Plugin ID: 20215
Timestamp: 2025-03-03 01:02:37
Port: 443

Plugin ID: 19426
Timestamp: 2025-03-03 01:01:31
Port: 443

Plugin ID: 109553
Timestamp: 2025-03-03 01:01:43
Port: 443

Plugin ID: 13841
Timestamp: 2025-03-03 01:01:30
Port: 443

Plugin ID: 11699
Timestamp: 2025-03-03 01:02:22
Port: 443

Plugin ID: 107225
Timestamp: 2025-03-03 01:02:14
Port: 443

Plugin ID: 10286
Timestamp: 2025-03-03 01:02:17
Port: 443

Plugin ID: 73895
Timestamp: 2025-03-03 01:02:03
Port: 443

Plugin ID: 66233
Timestamp: 2025-03-03 01:02:33
Port: 443

Plugin ID: 10645
Timestamp: 2025-03-03 01:01:50
Port: 443

Plugin ID: 11955
Timestamp: 2025-03-03 01:02:27
Port: 443

Plugin ID: 20317
Timestamp: 2025-03-03 01:02:02
Port: 443

Plugin ID: 55978
Timestamp: 2025-03-03 01:02:27
Port: 443

Plugin ID: 18287
Timestamp: 2025-03-03 01:01:45
Port: 443

Plugin ID: 10526
Timestamp: 2025-03-03 01:01:44
Port: 443
```

```
Plugin ID: 189227
Timestamp: 2025-03-03 01:02:32
Port: 443

Plugin ID: 11576
Timestamp: 2025-03-03 01:02:17
Port: 443

Plugin ID: 51456
Timestamp: 2025-03-03 01:02:39
Port: 443

Plugin ID: 18297
Timestamp: 2025-03-03 01:01:37
Port: 443

Plugin ID: 47619
Timestamp: 2025-03-03 01:02:21
Port: 443

Plugin ID: 23639
Timestamp: 2025-03-03 01:01:40
Port: 443

Plugin ID: 11706
Timestamp: 2025-03-03 01:02:21
Port: 443

Plugin ID: 69176
Timestamp: 2025-03-03 01:02:37
Port: 443

Plugin ID: 17608
Timestamp: 2025-03-03 01:01:29
Port: 443

Plugin ID: 194954
Ti [...]
```

## 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: 2022/09/09

### Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 54
```

## 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 :

1C:61:B4:AC:C8:6D : TP-Link Corporation Limited
```

## 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:
  - 1C:61:B4:AC:C8:6D
```

## 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

### Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

### Plugin Output

tcp/443/www

```
HTTP/1.1 200 OK
Connection: close
ETag: "20e-110-669a4d9a"
Last-Modified: Fri, 19 Jul 2024 11:27:22 GMT
Date: Mon, 03 Mar 2025 00:59:11 GMT
X-Frame-Options: deny
Content-Security-Policy: frame-ancestors 'none'
Content-Type: text/html
Content-Length: 272

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

## 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

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on tests of each method :

  - HTTP methods DELETE GET HEAD OPTIONS POST PUT are allowed on :

    /
    /cgi-bin
    /webpages
    /webpages/themes
    /webpages/themes/default
    /webpages/themes/default/css
```

## 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 is 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: 2024/02/26

### Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Connection: Keep-Alive
  Keep-Alive: timeout=20
  ETag: "20e-110-669a4d9a"
  Last-Modified: Fri, 19 Jul 2024 11:27:22 GMT
  Date: Mon, 03 Mar 2025 01:08:27 GMT
  X-Frame-Options: deny
  Content-Security-Policy: frame-ancestors 'none'
  Content-Type: text/html
  Content-Length: 272

Response Body :

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="refresh" content="0; URL=/webpages/index.html" />
```

```
</head>
</html>
```

## 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 is 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: 2024/02/26

### Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Connection: Keep-Alive
  Keep-Alive: timeout=20
  ETag: "20e-110-669a4d9a"
  Last-Modified: Fri, 19 Jul 2024 11:27:22 GMT
  Date: Mon, 03 Mar 2025 01:08:36 GMT
  X-Frame-Options: deny
  Content-Security-Policy: frame-ancestors 'none'
  Content-Type: text/html
  Content-Length: 272

Response Body :

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="refresh" content="0; URL=/webpages/index.html" />
```

```
</head>
</html>
```

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80/www

```
Request        : http://192.168.68.1/
HTTP response  : HTTP/1.1 200 OK
Redirect to    : http://192.168.68.1/webpages/index.html
Redirect type  : meta redirect

Request        : http://192.168.68.1/webpages/index.html
HTTP response  : HTTP/1.1 200 OK
Redirect to    : http://192.168.68.1/webpages/error.html
Redirect type  : meta redirect

Final page     : http://192.168.68.1/webpages/error.html
HTTP response  : HTTP/1.1 200 OK
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
4IP
6TCP
17UDP
41IPv6
47GRE
50ESP
51AH
108IPComp
115L2TP
136UDPLite
```

## 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.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202503021233
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : HAIDEN-HOME-NETWORK-SCAN
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.68.67
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 220.075 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/2 19:57 EST (UTC -05:00)
Scan duration : 3926 sec
Scan for malware : yes
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/53/dns

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

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/80/www

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

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/443/www

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

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/20001/ssh

```
Port 20001/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: 2024/10/14

### Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.x
Confidence level : 54
Method : SinFP


The remote host is running Linux Kernel 2.x
```

## 117886 - OS Security Patch Assessment Not Available

### Synopsis

OS Security Patch Assessment is not available.

### Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

### Solution

n/a

### Risk Factor

None

### References

XREF                IAVB:0001-B-0515

### Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

### Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SSH service.
```

## 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/20001/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

  Client to Server: aes256-ctr
  Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

  none

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha2-256
  hmac-sha2-512

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp521
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes256-ctr

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha2-256
  hmac-sha2-512
```

```
The server supports the following options for kex_algorithms :

  diffie-hellman-group14-sha256
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  kexguess2@matt.ucc.asn.au

The server supports the following options for compression_algorithms_client_to_server :

  none

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes256-ctr
```

## 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

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/20001/ssh

## 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.

### Solution

n/a

### Risk Factor

None

### References

XREF                IAVT:0001-T-0933

### Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

### Plugin Output

tcp/20001/ssh

```
SSH version : SSH-2.0-dropbear
SSH supported authentication : publickey,password
```

## 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: 2023/07/10

Plugin Output

tcp/443/www

```
This port supports SSLv2/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: 2021/02/03

### Plugin Output

tcp/443/www

```
Subject Name:

Country: CN
Common Name: tplinkdeco.net

Issuer Name:

Country: CN
Common Name: tplinkdeco.net

Serial Number: 00 B8 82 DA 79 82 56 9B D4

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 01 00:00:00 2010 GMT
Not Valid After: Dec 31 00:00:00 2030 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AB B1 86 4A 2D B8 CD B3 E1 F7 F1 E8 D6 49 AD 4E 0B 11 BF
            EE 74 28 59 EE 64 21 BE F8 1A 43 34 26 E4 10 0A 56 30 30 E8
            7C 92 F9 B1 41 D6 EA BE 22 44 C6 D2 F4 2B 43 9D F5 D6 E8 75
            1B 37 0E A1 92 ED DA 1A D0 99 C0 1E 76 DA 3A 20 6D 31 DE D7
            53 81 BD 09 35 7D 08 9C 50 0A 72 56 2F 8B CD FE DE C6 CD C6
            B2 76 04 8B 5A 7B 59 6E 1E 9A F8 BA 8C 19 A0 A0 84 65 2B BC
            88 AD 1B 31 31 C3 AD ED DF AF A5 28 A6 E8 EB ED 7E 16 AE B8
            E3 9B 86 42 0A E3 F8 C0 87 5E 77 D2 FE 5D B9 F6 2F 7D F3 25
            5E 63 35 96 46 30 A4 F7 49 D7 38 E2 AA DC 6C 79 52 46 AB 16
```

```
            CC AB B7 D6 0F F4 2C 37 47 08 3C 72 6B 56 40 B1 A2 27 5B AD
            B3 B9 13 EF 92 96 4F 4B BC 17 95 C9 20 9A 95 E8 55 37 5C EB
            83 3B 95 C2 77 71 AE 0B F3 86 6F 3B D4 97 2A 96 B2 02 20 21
            28 20 4C 5E 0C 92 79 C1 59 C1 CA AE 9E 72 01 3B B5
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 39 12 0D 53 7B 11 92 BB 6E 7C 8F A7 D1 0D 38 A5 46 B1 A7
            30 88 E4 B7 90 A2 31 18 6E 85 C0 C6 D3 33 C6 75 2F A0 D8 70
            EC 45 6F 30 E9 07 D0 CA 25 A6 F5 3D 6E CC 6C A8 41 BF 91 27
            26 FD 28 CE F5 30 D3 DB 89 4D C5 10 36 DB 2F B1 33 2A 99 63
            A3 18 2A B5 F1 55 35 18 FA E8 1E C1 F6 6D D9 36 76 25 93 A6
            89 AB E2 1B E3 79 6E 69 27 56 E9 26 06 71 89 7C 65 24 8C DD
            95 D6 DD 6B 87 93 DA B6 66 61 9E 06 25 4C 5E E9 C4 D9 E0 20
            CD E0 FA 7D CA 9A A3 C6 A4 CD E2 2C 8A 50 A1 5A BB BE FE 8F
            20 F7 6D D6 E2 1D E9 19 F3 48 D8 A9 29 71 0B 75 B6 96 D0 EF
            B4 3C CA C5 C6 01 [...]
```

## 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: 2024/03/26

Plugin Output

tcp/80/www

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

## 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: 2024/03/26

Plugin Output

tcp/443/www

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

tcp/443/www

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

Plugin Output

tcp/20001/ssh

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

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

Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

Plugin Output

tcp/0

## 117860 - TP-Link HTTP Server Detection

Synopsis

It is possible to fingerprint the remote TP-Link HTTP server.

Description

The remote host has an accessible TP-Link HTTP administrative page.

It is possible to determine the model information from the host.

Note: In some instances, it may be possible to identify the device firmware version.

See Also

https://www.tp-link.com/us/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/10/01, Modified: 2025/02/12

Plugin Output

tcp/80/www

```
URL     : http://192.168.68.1/
Version : unknown
```

## 110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF                IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

```
SSH was detected on port 20001 but no credentials were provided.
SSH local checks were not enabled.
```

## 10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.68.67 to 192.168.68.1 :
192.168.68.67
192.168.68.1

Hop Count: 1
```

## 91815 - Web Application Sitemap

### Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

### Description

The remote web server contains linkable content that can be used to gather information about a target.

### See Also

http://www.nessus.org/u?5496c8d9

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

### Plugin Output

tcp/80/www

```
 The following sitemap was created from crawling linkable content on the target host :

   - http://192.168.68.1/
   - http://192.168.68.1/webpages/
   - http://192.168.68.1/webpages/error.html
   - http://192.168.68.1/webpages/favicon.ico
   - http://192.168.68.1/webpages/index.html
   - http://192.168.68.1/webpages/themes/default/css/perfect-scrollbar.css
   - http://192.168.68.1/webpages/themes/default/css/total.css

 Attached is a copy of the sitemap file.
```

## 11032 - Web Server Directory Enumeration

### Synopsis

It is possible to enumerate directories on the web server.

### Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

### See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

### Solution

n/a

### Risk Factor

None

### References

XREF              OWASP:OWASP-CM-006

### Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

### Plugin Output

tcp/80/www

```
The following directories were discovered:
/cgi-bin

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

# 192.168.68.50

| 0 | 0 | 0 | 0 | 7 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |
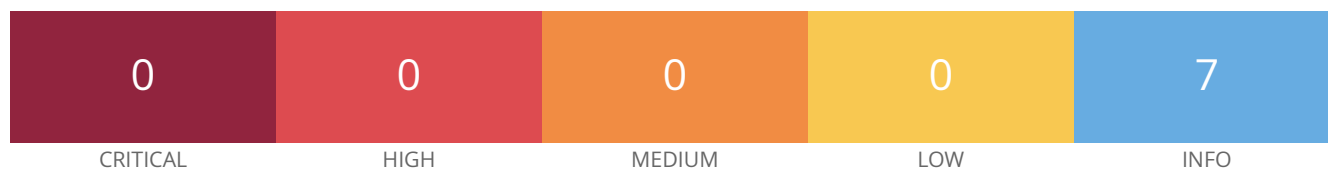
## Scan Information

Start time:     Sun Mar 2 19:57:28 2025
End time:       Sun Mar 2 20:00:30 2025

## Host Information

IP:             192.168.68.50
MAC Address:    DC:4F:22:EF:14:06

## Vulnerabilities

### 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

## Plugin Output

tcp/0

```
The following card manufacturers were identified :

DC:4F:22:EF:14:06 : Espressif 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:
  - DC:4F:22:EF:14:06
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
```

## 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.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

### Plugin Output

tcp/0

```
 Information about this scan :

 Nessus version : 10.8.3
 Nessus build : 20010
 Plugin feed version : 202503021233
 Scanner edition used : Nessus Home
 Scanner OS : LINUX
 Scanner distribution : ubuntu1604-x86-64
 Scan type : Normal
 Scan name : HAIDEN-HOME-NETWORK-SCAN
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.68.67
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 280.722 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/2 19:57 EST (UTC -05:00)
Scan duration : 177 sec
Scan for malware : yes
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/6668

```
Port 6668/tcp was found to be open
```

## 50350 - OS Identification Failed

### Synopsis

It was not possible to determine the remote operating system.

### Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. Unfortunately, though, Nessus does not currently know how to use them to identify the overall system.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2024/09/30

### Plugin Output

tcp/0

```
If you think that these signatures would help us improve OS fingerprinting,
please submit them by visiting https://www.tenable.com/research/submitsignatures.

ICMP:!::1:S:1:255:0::1:0:::0::1:8:255:0:1:1:2:1:1:1:0:1:255:4380:M:N:N:N
SinFP:!:
   P1:B11013:F0x12:W4380:O0204ffff:M1460:
   P2:B11013:F0x12:W4380:O0204ffff:M1460:
   P3:B00000:F0x00:W0:O0:M0
   P4:191003_7_p=6668
```

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.68.67 to 192.168.68.50 :
192.168.68.67
192.168.68.50

Hop Count: 1
```

# 192.168.68.51

| 0 | 0 | 0 | 0 | 8 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |
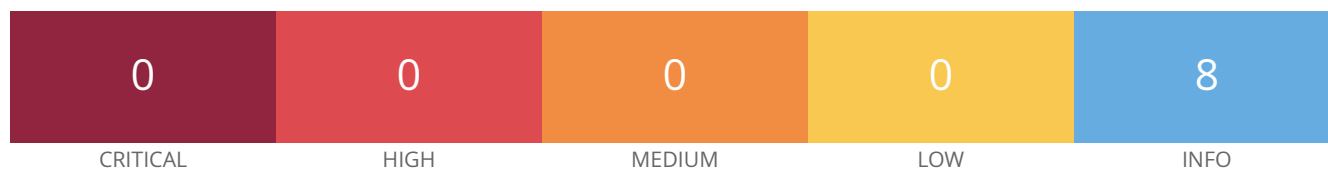
## Scan Information

Start time:     Sun Mar 2 19:57:28 2025

End time:     Sun Mar 2 20:00:38 2025

## Host Information

IP:     192.168.68.51

MAC Address:     50:91:E3:8A:99:24

OS:     EthernetBoard OkiLAN 8100e

## Vulnerabilities

### 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: 2022/09/09

#### Plugin Output

tcp/0

```
Remote device type : switch
Confidence level : 65
```

## 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 :

50:91:E3:8A:99:24 : TP-Link Corporation Limited
```

## 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:
  - 50:91:E3:8A:99:24
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
```

## 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202503021233
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : HAIDEN-HOME-NETWORK-SCAN
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.68.67
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 1283.374 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/2 19:57 EST (UTC -05:00)
Scan duration : 182 sec
Scan for malware : yes
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/9999

```
Port 9999/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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : EthernetBoard OkiLAN 8100e
Confidence level : 65
Method : SinFP


The remote host is running EthernetBoard OkiLAN 8100e
```

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.68.67 to 192.168.68.51 :
192.168.68.67
192.168.68.51

Hop Count: 1
```

# 192.168.68.52

| 0 | 0 | 0 | 0 | 8 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

## Scan Information

Start time:      Sun Mar 2 19:57:28 2025
End time:        Sun Mar 2 20:00:51 2025

## Host Information

IP:              192.168.68.52
MAC Address:     78:8C:B5:F0:77:A7
OS:              EthernetBoard OkiLAN 8100e

## Vulnerabilities

### 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: 2022/09/09

#### Plugin Output

tcp/0

```
Remote device type : switch
Confidence level : 65
```

## 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 :

78:8C:B5:F0:77:A7 : TP-Link Corporation Limited
```

## 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:
  - 78:8C:B5:F0:77:A7
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
```

## 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.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

### Plugin Output

tcp/0

```
 Information about this scan :

 Nessus version : 10.8.3
 Nessus build : 20010
 Plugin feed version : 202503021233
 Scanner edition used : Nessus Home
 Scanner OS : LINUX
 Scanner distribution : ubuntu1604-x86-64
 Scan type : Normal
 Scan name : HAIDEN-HOME-NETWORK-SCAN
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.68.67
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 220.968 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/2 19:57 EST (UTC -05:00)
Scan duration : 195 sec
Scan for malware : yes
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/9999

```
Port 9999/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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : EthernetBoard OkiLAN 8100e
Confidence level : 65
Method : SinFP


The remote host is running EthernetBoard OkiLAN 8100e
```

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.68.67 to 192.168.68.52 :
192.168.68.67
192.168.68.52

Hop Count: 1
```

# 192.168.68.54

| 0 | 1 | 4 | 1 | 53 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

## Scan Information

Start time:        Sun Mar 2 19:57:28 2025
End time:         Sun Mar 2 20:27:39 2025

## Host Information

IP:            192.168.68.54
MAC Address:    38:86:F7:B3:25:84
OS:          Linux Kernel 2.6

## Vulnerabilities

### 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

http://www.nessus.org/u?df5555f5

https://sweet32.info

#### Solution

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

#### Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

EPSS Score

0.0398

CVSS v2.0 Base Score

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

References

CVE                 CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/8009

```
  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}
```

## 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 v2.0 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/8009

```
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=76994d09-9c6e-e0f2-a463-d952cee3ef45
|-Issuer  : CN=76994d09-9c6e-e0f2-a463-d952cee3ef45
```

## 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 v2.0 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/8443/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 : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Chromecast ICA 21 (ATV)
|-Issuer  : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Cast Root CA
```

## 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 v2.0 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/10001

```
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 : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Chromecast ICA 21 (ATV)
|-Issuer  : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Cast Root CA
```

## 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.

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 v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/8009

```
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=76994d09-9c6e-e0f2-a463-d952cee3ef45
```

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.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.8939

CVSS v2.0 Base Score

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

References

| | |
|------|-------------|
| CVE | CVE-1999-0524 |
| XREF | CWE:200 |

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

## 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: 2025/02/12

## Plugin Output

tcp/0

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

    cpe:/o:linux:linux_kernel -> Linux Kernel
```

## 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: 2022/09/09

### Plugin Output

tcp/0

```
Remote device type : unknown
Confidence level : 56
```

## 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 :

38:86:F7:B3:25:84 : Google, 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:
  - 38:86:F7:B3:25:84
```

## 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

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/8443/www

```
HTTP/1.1 404 Not Found
Content-Length:0
Content-Type:text/html

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

## 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

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/8008/www

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
    INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 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

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/8443/www

```
Based on tests of each method :

   - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
     BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
     INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
     OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
     RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
     UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

     /

   - Invalid/unknown HTTP methods are allowed on :

     /
```

## 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 is 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: 2024/02/26

## Plugin Output

tcp/8008/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Length:0
  Content-Type:text/html

Response Body :
```

## 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 is 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: 2024/02/26

### Plugin Output

tcp/8443/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Length:0
  Content-Type:text/html

Response Body :
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
4IP
6TCP
17UDP
41IPv6
47GRE
50ESP
51AH
108IPComp
115L2TP
136UDPLite
```

## 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.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202503021233
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : HAIDEN-HOME-NETWORK-SCAN
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.68.67
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 165.985 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/2 19:57 EST (UTC -05:00)
Scan duration : 1806 sec
Scan for malware : yes
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/8008/www

```
Port 8008/tcp was found to be open
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/8009

```
Port 8009/tcp was found to be open
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/8443/www

```
Port 8443/tcp was found to be open
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/9000

```
Port 9000/tcp was found to be open
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/10001

```
Port 10001/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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6
Confidence level : 56
Method : MLSinFP


The remote host is running Linux Kernel 2.6
```

## 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.

### Solution

Steps to resolve this issue include :

- 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

### Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

### Plugin Output

tcp/0

```
Port 10001 was detected as being open but is now closed
```

## 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: 2023/07/10

Plugin Output

tcp/8009

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

## 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: 2023/07/10

Plugin Output

tcp/8443/www

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

## 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: 2023/07/10

Plugin Output

tcp/10001

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

## 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.

### Solution

Renew any soon to expire SSL certificates.

### Risk Factor

None

### Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

### Plugin Output

tcp/8009

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject    : CN=76994d09-9c6e-e0f2-a463-d952cee3ef45
|-Not After : Mar 03 19:57:08 2025 GMT
```

## 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.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

Plugin Output

tcp/8009

```
The SSL certificate will expire within 60 days, at
Mar  3 19:57:08 2025 GMT :

  Subject          : CN=76994d09-9c6e-e0f2-a463-d952cee3ef45
  Issuer           : CN=76994d09-9c6e-e0f2-a463-d952cee3ef45
  Not valid before : Mar  1 19:57:08 2025 GMT
  Not valid after  : Mar  3 19:57:08 2025 GMT
```

## 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: 2021/02/03

### Plugin Output

tcp/8009

```
Subject Name:

Common Name: 76994d09-9c6e-e0f2-a463-d952cee3ef45

Issuer Name:

Common Name: 76994d09-9c6e-e0f2-a463-d952cee3ef45

Serial Number: 15 32 DA 5C

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Mar 01 19:57:08 2025 GMT
Not Valid After: Mar 03 19:57:08 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 EC EA D8 AA 8F 17 03 EF 1E 1F 01 22 1F 5F DB 6A D5 DB 37
            17 7A D3 B7 62 02 5C 10 4E E5 E4 04 0E 81 2E EE 84 6A 9D 9D
            8D DF 74 BC C6 AA D5 65 A5 F8 1C 83 50 6B DF 87 DC 0C 5E 92
            5B B0 F7 5D DC BD 70 94 62 C6 9B 3C 20 28 86 84 2A 4C 2A E8
            2E E0 DF 44 06 AA 75 43 21 34 52 19 80 92 BE 3C DA D2 14 B7
            91 68 74 C5 9E 3A EE E4 7F 88 54 AC 5C F3 6A 0F 41 EB 95 94
            90 F3 80 47 4C 06 0A 73 A8 1B CF C6 0B 8D EA 6D DA 45 97 BD
            6C 50 C9 C0 11 C7 7C B6 DB F2 D7 BD 22 0B 76 DC 7D EF DC F3
            B5 04 0F A5 23 50 F8 F7 CE 27 A5 DA 00 CB 69 6A B3 AA BD 24
            C8 9C 29 5D 61 05 39 8F 6D 61 53 DD 4D 0E D5 9E 6B F5 25 71
            1B 81 3E 5C 60 B1 E3 7E B1 79 12 C3 38 12 74 C5 33 0F 37 61
```

```
              19 6E C6 BA E0 E1 C3 E3 40 95 74 AB C3 38 3C 4E 76 D4 99 EF
              B8 5E 28 D0 31 9B AB E7 D7 D6 80 C2 59 F5 E0 9A A5
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 0A C8 F2 4A 0A CC 21 16 80 FC CF 2C 94 B7 1C EA 34 49 09
           B1 1F 0A EA C0 33 95 B9 4E 48 6E C2 97 D3 41 C2 60 39 22 0F
           26 7B 0E 50 79 50 81 DD DE 2E 95 B1 07 EA BD B4 58 3F 8C B8
           91 F6 87 26 79 81 FC 86 6B 23 F2 9B 21 1B 81 94 4F 4F 96 42
           DE 28 AD D7 6E B5 53 89 DA 05 B3 E9 45 A9 F2 04 E8 33 7B 34
           A2 74 E0 5B 98 95 92 BE 8D 45 F0 B0 3F BB 1E 06 36 09 9E 24
           7A F9 93 B9 85 81 7A 60 7F E1 15 F1 BB 7A 6B 32 50 B1 D2 24
           D4 16 6C D4 D6 8A 6A C0 62 9A E5 48 A5 1E B4 66 6E 6B 69 45
           D1 1D 0A E9 F1 96 FC 07 2D 2C 2E E5 E0 1C 16 DC 48 DE BB 63
           B6 0D 2A 2C  [...]
```

## 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: 2021/02/03

Plugin Output

tcp/8443/www

```
Subject Name:

Country: US
State/Province: California
Locality: Mountain View
Organization: Google Inc
Organization Unit: Cast
Common Name: DD8LDUK FA8FCA72C38C

Issuer Name:

Country: US
State/Province: California
Locality: Mountain View
Organization: Google Inc
Organization Unit: Cast
Common Name: Chromecast ICA 21 (ATV)

Serial Number: 44 44 38 4C 44 55 4B

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Mar 05 08:00:00 2019 GMT
Not Valid After: Oct 13 23:32:46 2042 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A0 F9 1A 66 F8 15 66 70 58 52 6A D5 78 13 50 F1 A5 51 2D
```

```
            0B 72 FA 68 61 B3 6D 1A 9F 6C 86 26 73 22 2D 45 8B 01 AA 69
            EB E6 D7 38 14 E1 F2 47 75 AD 19 9B AA C2 CE 79 77 18 CD C1
            D5 52 87 26 A8 62 F9 6F 12 A4 3F B5 AE B1 EC FF 59 C2 6B FE
            B7 5C 16 61 D6 DF 6D 6F 88 B5 D2 30 7B C9 A9 E9 42 37 59 0B
            C0 35 5C 08 7A 82 2A 76 E0 15 D9 CF 0E 23 64 7C 0E 0C 19 E0
            F2 2B 6D 84 F4 1B B4 30 2C 6E B6 6A 95 3E 54 4A AB 3A DE FA
            BD 9A 71 B5 B5 E1 3A 8E E7 38 9A EA 06 39 F8 BC F5 3A E8 67
            7E D9 DA B5 52 27 99 87 2D C7 DE 67 86 71 6E BB 6C E8 48 4C
            B1 4E 79 37 0D 94 87 69 0A 82 62 20 45 A9 BA 4A 25 10 F8 60
            55 14 AF AD 83 1A CA CF 4F AC 4E E1 DF 68 58 C7 D3 07 84 D3
            9C BB 42 04 C2 4A AC C5 8E 20 E1 9C 59 6F F7 7E 5B 12 BC A6
            7F 41 DE 3B 31 43 E5 28 D4 80 E9 25 BA BF 52 EF B5
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 55 82 5F F4 C2 44 79 2D C4 D4 CC 8C 5C 39 D3 C8 EF A0 70
            7E 36 50 E3 EE F3 2A A6 58 57 A6 35 8C 04 7D A4 8C A2 A3 BB
            37 E5 57 A6 EB E2 E8 B3 A8 18 A9 14 81 15 A0 0E 0F C7 66 53
            70 AE 79 82 44 F9 0C 64 6F 97 41 1C F4 36 40 7A 43 BB 26 A4
            B0 00 EC AF 8F 6E E1 57 A8 E2 81 DC ED F8 0C DD 3E D2 2C 09
            75 8D 12 F9 9B 3D 1B 02 38 B8 86 65 1D 31 8D A8 A9 E0 2B 90
            25 01 10 04 39 F7 51 1A  [...]
```

## 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: 2021/02/03

Plugin Output

tcp/10001

```
Subject Name:

Country: US
State/Province: California
Locality: Mountain View
Organization: Google Inc
Organization Unit: Cast
Common Name: DD8LDUK FA8FCA72C38C

Issuer Name:

Country: US
State/Province: California
Locality: Mountain View
Organization: Google Inc
Organization Unit: Cast
Common Name: Chromecast ICA 21 (ATV)

Serial Number: 44 44 38 4C 44 55 4B

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Mar 05 08:00:00 2019 GMT
Not Valid After: Oct 13 23:32:46 2042 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A0 F9 1A 66 F8 15 66 70 58 52 6A D5 78 13 50 F1 A5 51 2D
```

```
            0B 72 FA 68 61 B3 6D 1A 9F 6C 86 26 73 22 2D 45 8B 01 AA 69
            EB E6 D7 38 14 E1 F2 47 75 AD 19 9B AA C2 CE 79 77 18 CD C1
            D5 52 87 26 A8 62 F9 6F 12 A4 3F B5 AE B1 EC FF 59 C2 6B FE
            B7 5C 16 61 D6 DF 6D 6F 88 B5 D2 30 7B C9 A9 E9 42 37 59 0B
            C0 35 5C 08 7A 82 2A 76 E0 15 D9 CF 0E 23 64 7C 0E 0C 19 E0
            F2 2B 6D 84 F4 1B B4 30 2C 6E B6 6A 95 3E 54 4A AB 3A DE FA
            BD 9A 71 B5 B5 E1 3A 8E E7 38 9A EA 06 39 F8 BC F5 3A E8 67
            7E D9 DA B5 52 27 99 87 2D C7 DE 67 86 71 6E BB 6C E8 48 4C
            B1 4E 79 37 0D 94 87 69 0A 82 62 20 45 A9 BA 4A 25 10 F8 60
            55 14 AF AD 83 1A CA CF 4F AC 4E E1 DF 68 58 C7 D3 07 84 D3
            9C BB 42 04 C2 4A AC C5 8E 20 E1 9C 59 6F F7 7E 5B 12 BC A6
            7F 41 DE 3B 31 43 E5 28 D4 80 E9 25 BA BF 52 EF B5
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 55 82 5F F4 C2 44 79 2D C4 D4 CC 8C 5C 39 D3 C8 EF A0 70
            7E 36 50 E3 EE F3 2A A6 58 57 A6 35 8C 04 7D A4 8C A2 A3 BB
            37 E5 57 A6 EB E2 E8 B3 A8 18 A9 14 81 15 A0 0E 0F C7 66 53
            70 AE 79 82 44 F9 0C 64 6F 97 41 1C F4 36 40 7A 43 BB 26 A4
            B0 00 EC AF 8F 6E E1 57 A8 E2 81 DC ED F8 0C DD 3E D2 2C 09
            75 8D 12 F9 9B 3D 1B 02 38 B8 86 65 1D 31 8D A8 A9 E0 2B 90
            25 01 10 04 39 F7 51 1A  [...]
```

## 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: 2021/02/03

### Plugin Output

tcp/8009

```
  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
      --------------------        ----------    ---         ----    --------------------    ---
      ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH        RSA     AES-CBC(128)
    SHA1
      ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH        RSA     AES-CBC(256)
    SHA1
```

```
     AES128-SHA                    0x00, 0x2F      RSA           RSA        AES-CBC(128)
  SHA1
     AES256-SHA                    0x00, 0x35      RSA           RSA        AES-CBC(256)
  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}
```

## 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: 2021/02/03

### Plugin Output

tcp/8443/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

 The fields above are :

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

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

## 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: 2021/02/03

### Plugin Output

tcp/10001

```
  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

  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/man1.0.2/man1/ciphers.html

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/8009

```
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
  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
    --------------------          ----------    ---       ----    --------------------   ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F    ECDH      RSA     AES-GCM(128)
SHA256
    ECDHE-RSA-CHACHA20-POLY1305    0xCC, 0xA8    ECDH      RSA     ChaCha20-Poly1305(256)
SHA256
    RSA-AES128-SHA256             0x00, 0x9C    RSA       RSA     AES-GCM(128)
SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13    ECDH      RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14    ECDH      RSA     AES-CBC(256)
SHA1
    AES128-SHA                    0x00, 0x2F    RSA       RSA     AES-CBC(128)
SHA1
    AES256-SHA                    0x00, 0x35    RSA       RSA     AES-CBC(256)
SHA1


The fields ab [...]
```

## 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

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/8443/www

```
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
    --------------------          ----------    ---         ----     --------------------  ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F    ECDH        RSA      AES-GCM(128)
  SHA256
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8    ECDH        RSA      ChaCha20-Poly1305(256)
  SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13    ECDH        RSA      AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14    ECDH        RSA      AES-CBC(256)
  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}
```

## 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

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/10001

```
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
    --------------------        ----------    ---        ----    --------------------  ---
    ECDHE-RSA-AES128-SHA256     0xC0, 0x2F    ECDH       RSA     AES-GCM(128)
SHA256
    ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8    ECDH       RSA     ChaCha20-Poly1305(256)
SHA256
    ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH       RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH       RSA     AES-CBC(256)
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

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/8009

```
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-CHACHA20-POLY1305 0xCC, 0xA8    ECDH       RSA     ChaCha20-Poly1305(256)
SHA256
    ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH       RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH       RSA     AES-CBC(256)
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

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/8443/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-CHACHA20-POLY1305 0xCC, 0xA8   ECDH      RSA     ChaCha20-Poly1305(256)
  SHA256
     ECDHE-RSA-AES128-SHA        0xC0, 0x13   ECDH      RSA     AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA        0xC0, 0x14   ECDH      RSA     AES-CBC(256)
  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

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/10001

```
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-CHACHA20-POLY1305   0xCC, 0xA8    ECDH        RSA     ChaCha20-Poly1305(256)
SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13    ECDH        RSA     AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14    ECDH        RSA     AES-CBC(256)
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}
```

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/8009

```
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
    ECDHE-RSA-AES128-SHA         0xC0, 0x13  ECDH      RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA         0xC0, 0x14  ECDH      RSA      AES-CBC(256)
SHA1
    AES128-SHA                   0x00, 0x2F  RSA       RSA      AES-CBC(128)
SHA1
    AES256-SHA                   0x00, 0x35  RSA       RSA      AES-CBC(256)
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}
```

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/8443/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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

The fields above are :

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

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/10001

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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

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: 2024/03/26

Plugin Output

tcp/8009

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

## 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: 2024/03/26

Plugin Output

tcp/8443/www

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

## 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: 2024/03/26

Plugin Output

tcp/9000

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

## 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: 2024/03/26

Plugin Output

tcp/10001

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

## 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

**Plugin Information**

Published: 2007/05/16, Modified: 2023/10/17

**Plugin Output**

tcp/0

## 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/8009

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

## 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/8443/www

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

## 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/10001

```
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: 2023/12/13

Plugin Output

tcp/8009

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

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.68.67 to 192.168.68.54 :
192.168.68.67
192.168.68.54

Hop Count: 1
```

## 35711 - Universal Plug and Play (UPnP) Protocol Detection

Synopsis

The remote device supports UPnP.

Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

See Also

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

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

http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt

Solution

Filter access to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2018/09/12

Plugin Output

udp/1900/ssdp

```
 The device responded to an SSDP M-SEARCH request with the following locations :

     http://192.168.68.54:8008/ssdp/device-desc.xml

 And advertises these unique service names :

     uuid:76994d09-9c6e-e0f2-a463-d952cee3ef45::upnp:rootdevice
     uuid:76994d09-9c6e-e0f2-a463-d952cee3ef45::urn:dial-multiscreen-org:device:dial:1
     uuid:76994d09-9c6e-e0f2-a463-d952cee3ef45::urn:dial-multiscreen-org:service:dial:1
```

## 40405 - Web Server Detection (HTTP/1.1)

**Synopsis**

A web server is running on this port.

**Description**

The web server on this port responds to HTTP/1.1 requests and appears to ignore HTTP/1.0 requests, which is unusual.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2009/07/28, Modified: 2019/11/22

**Plugin Output**

tcp/8008/www

## 40405 - Web Server Detection (HTTP/1.1)

Synopsis

A web server is running on this port.

Description

The web server on this port responds to HTTP/1.1 requests and appears to ignore HTTP/1.0 requests, which is unusual.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2019/11/22

Plugin Output

tcp/8443/www

## 35712 - Web Server UPnP Detection

Synopsis

The remote web server provides UPnP information.

Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

See Also

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

Solution

Filter incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/06/12

Plugin Output

tcp/8008/www

```
Here is a summary of http://192.168.68.54:8008/ssdp/device-desc.xml :

deviceType: urn:dial-multiscreen-org:device:dial:1
friendlyName: Master Bedroom TV
manufacturer: Google
modelName: Eureka Dongle
modelName: Eureka Dongle
ServiceID: urn:dial-multiscreen-org:serviceId:dial
serviceType: urn:dial-multiscreen-org:service:dial:1
controlURL: /ssdp/notfound
eventSubURL: /ssdp/notfound
SCPDURL: /ssdp/notfound
```

## 66717 - mDNS Detection (Local Network)

### Synopsis

It is possible to obtain information about the remote host.

### Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

### Solution

Filter incoming traffic to UDP port 5353, if desired.

### Risk Factor

None

### Plugin Information

Published: 2013/05/31, Modified: 2013/05/31

### Plugin Output

udp/5353/mdns

```
Nessus was able to extract the following information :

  - mDNS hostname       : Android-2.local.

  - Advertised services :
    o Service name      : Master Bedroom TV._androidtvremote2._tcp.local.
      Port number       : 6466
```

# 192.168.68.55

| 0 | 0 | 0 | 0 | 8 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |
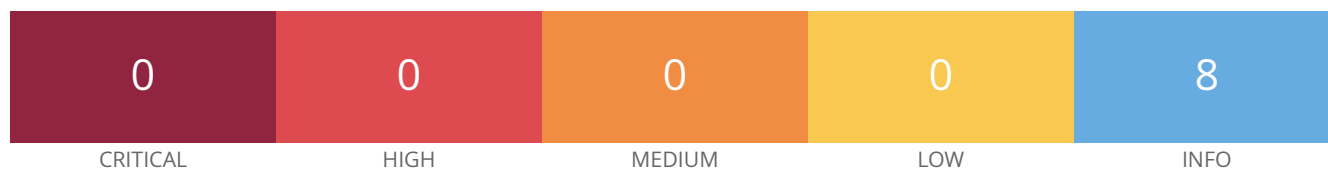
## Scan Information

Start time:  Sun Mar 2 19:57:29 2025

End time:  Sun Mar 2 20:01:07 2025

## Host Information

IP:  192.168.68.55

MAC Address:  D8:44:89:90:5F:03

OS:  EthernetBoard OkiLAN 8100e

## Vulnerabilities

### 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: 2022/09/09

#### Plugin Output

tcp/0

```
Remote device type : switch
Confidence level : 65
```

## 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 :

  D8:44:89:90:5F:03 : TP-LINK CORPORATION PTE. LTD.
```

## 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:
  - D8:44:89:90:5F:03
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
6TCP
17UDP
```

## 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202503021233
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : HAIDEN-HOME-NETWORK-SCAN
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.68.67
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 182.446 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/2 19:57 EST (UTC -05:00)
Scan duration : 213 sec
Scan for malware : yes
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/9999

```
Port 9999/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: 2024/10/14

### Plugin Output

tcp/0

```
Remote operating system : EthernetBoard OkiLAN 8100e
Confidence level : 65
Method : SinFP


The remote host is running EthernetBoard OkiLAN 8100e
```

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

### Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.68.67 to 192.168.68.55 :
192.168.68.67
192.168.68.55

Hop Count: 1
```

# 192.168.68.56

| 0 | 1 | 17 | 1 | 74 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |
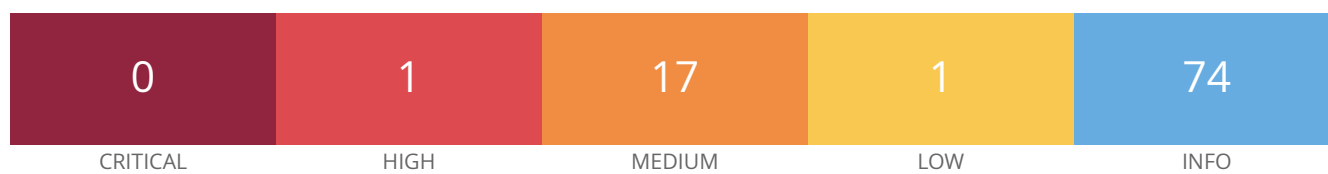
## Scan Information

Start time:        Sun Mar 2 19:57:29 2025
End time:          Sun Mar 2 20:26:04 2025

## Host Information

IP:                192.168.68.56
MAC Address:       84:B8:B8:36:B2:F7
OS:                Linux Kernel 2.6

## Vulnerabilities

**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

http://www.nessus.org/u?df5555f5

https://sweet32.info

### Solution

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

### Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

5.1

EPSS Score

0.0398

CVSS v2.0 Base Score

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

References

CVE             CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2025/02/12

Plugin Output

tcp/8009

```
  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}
```

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 v2.0 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/8009

```
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=35b14527-b650-4766-36ac-2158f68f9c3a
|-Issuer  : CN=35b14527-b650-4766-36ac-2158f68f9c3a
```

## 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 v2.0 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/8443/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 : C=US/O=Google Inc./OU=Android Things/CN=Android Things Cast Intermediate CA
|-Issuer  : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Cast Root CA
```

## 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 v2.0 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/9000

```
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 : C=US/O=Google Inc./OU=Android Things/CN=Android Things Cast Intermediate CA
|-Issuer  : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Cast Root CA
```

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 v2.0 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/10001

```
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 : C=US/O=Google Inc./OU=Android Things/CN=Android Things Cast Intermediate CA
|-Issuer  : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Cast Root CA
```

## 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 v2.0 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/10101

```
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 : C=US/O=Google Inc./OU=Android Things/CN=Android Things Cast Intermediate CA
|-Issuer  : C=US/ST=California/L=Mountain View/O=Google Inc/OU=Cast/CN=Cast Root CA
```

## 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.

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 v2.0 Base Score

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

Plugin Information

Published: 2012/01/17, Modified: 2022/06/14

Plugin Output

tcp/8009

```
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=35b14527-b650-4766-36ac-2158f68f9c3a
```

## 58751 - SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

### Synopsis

It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

### Description

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data.

If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled.

Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

### See Also

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

https://www.imperialviolet.org/2011/09/23/chromeandbeast.html

https://vnhacker.blogspot.com/2011/09/beast.html

http://www.nessus.org/u?649b81c1

http://www.nessus.org/u?84775fd6

https://blogs.msdn.microsoft.com/kaushal/2012/01/20/fixing-the-beast/

### Solution

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.

Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## VPR Score

2.9

## EPSS Score

0.0143

## CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

## CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## STIG Severity

I

## References

| | |
|---|---|
| BID | 49778 |
| CVE | CVE-2011-3389 |
| XREF | CERT:864643 |
| XREF | MSFT:MS12-006 |
| XREF | IAVB:2012-B-0006 |
| XREF | CEA-ID:CEA-2019-0547 |

## Plugin Information

Published: 2012/04/16, Modified: 2025/02/11

## Plugin Output

tcp/8443/www

```
Negotiated cipher suite: ECDHE-RSA-AES128-SHA|TLSv1|ECDH|RSA|AES-CBC(128)|SHA1
```

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

## tcp/8009

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

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

## tcp/8443/www

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

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

## tcp/9000

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

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

## tcp/10001

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

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19

Plugin Output

## tcp/10101

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

## 157288 - TLS Version 1.1 Deprecated Protocol

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://datatracker.ietf.org/doc/html/rfc8996

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

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/8009

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

## 157288 - TLS Version 1.1 Deprecated Protocol

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://datatracker.ietf.org/doc/html/rfc8996

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

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/8443/www

TLSv1.1 is enabled and the server supports at least one cipher.

## 157288 - TLS Version 1.1 Deprecated Protocol

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://datatracker.ietf.org/doc/html/rfc8996

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

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/9000

TLSv1.1 is enabled and the server supports at least one cipher.

## 157288 - TLS Version 1.1 Deprecated Protocol

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://datatracker.ietf.org/doc/html/rfc8996

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

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/10001

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

## 157288 - TLS Version 1.1 Deprecated Protocol

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://datatracker.ietf.org/doc/html/rfc8996

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

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF                CWE:327

Plugin Information

Published: 2022/04/04, Modified: 2024/05/14

Plugin Output

tcp/10101

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

## 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.

Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor

Low

VPR Score

2.2

EPSS Score

0.8939

CVSS v2.0 Base Score

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

References

CVE                CVE-1999-0524
XREF               CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

## 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: 2025/02/12

### Plugin Output

tcp/0

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

  cpe:/o:linux:linux_kernel -> Linux Kernel
```

## 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: 2022/09/09

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

## 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 :

84:B8:B8:36:B2:F7 : Motorola (Wuhan) Mobility Technologies Communication Co., Ltd.
```

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:
  - 84:B8:B8:36:B2:F7
```

## 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

Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

Plugin Output

tcp/8443/www

```
HTTP/1.1 404 Not Found
Content-Length:0
Content-Type:text/html

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

## 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

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/8008/www

```
Based on tests of each method :

   - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
     BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
     INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
     OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
     RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
     UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

       /

   - Invalid/unknown HTTP methods are allowed on :

       /
```

## 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

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/8443/www

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
    INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 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 is 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: 2024/02/26

### Plugin Output

tcp/8008/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Length:0
  Content-Type:text/html

Response Body :
```

## 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 is 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: 2024/02/26

### Plugin Output

tcp/8443/www

```
Response Code : HTTP/1.1 404 Not Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Content-Length:0
  Content-Type:text/html

Response Body :
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
4IP
6TCP
17UDP
41IPv6
50ESP
51AH
103PIM
108IPComp
136UDPLite
```

## 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.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2024/12/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.3
Nessus build : 20010
Plugin feed version : 202503021233
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : HAIDEN-HOME-NETWORK-SCAN
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.68.67
Port scanner(s) : nessus_tcp_scanner
Port range : default
Ping RTT : 191.019 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/2 19:57 EST (UTC -05:00)
Scan duration : 1710 sec
Scan for malware : yes
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/8008/www

```
Port 8008/tcp was found to be open
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/8009

```
Port 8009/tcp was found to be open
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/8443/www

```
Port 8443/tcp was found to be open
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/9000

```
Port 9000/tcp was found to be open
```

## 10335 - Nessus TCP scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

### Plugin Output

tcp/10001

```
Port 10001/tcp was found to be open
```

## 10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.

Once a TCP connection is open, it grabs any available banner for the service identification plugins.

Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/02/12

Plugin Output

tcp/10101

```
Port 10101/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: 2024/10/14

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

## 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.

Solution

Steps to resolve this issue include :

- 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

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

tcp/0

```
Port 10101 was detected as being open but is now closed
Port 10001 was detected as being open but is now closed
Port 9000 was detected as being open but is now closed
```

## 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

### Plugin Information

Published: 2010/11/30, Modified: 2020/06/12

### Plugin Output

tcp/8009

## 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: 2023/07/10

Plugin Output

tcp/8009

```
This port supports TLSv1.3/TLSv1.0/TLSv1.1/TLSv1.2.
```

## 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: 2023/07/10

Plugin Output

tcp/8443/www

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

## 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: 2023/07/10

Plugin Output

tcp/9000

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

## 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: 2023/07/10

**Plugin Output**

tcp/10001

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

## 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: 2023/07/10

Plugin Output

tcp/10101

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

## 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.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/8009

```
The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=35b14527-b650-4766-36ac-2158f68f9c3a
|-Not After : Mar 04 06:29:18 2025 GMT
```

## 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.

### Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

### Risk Factor

None

### Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

### Plugin Output

tcp/8009

```
 The SSL certificate will expire within 60 days, at
 Mar  4 06:29:18 2025 GMT :

   Subject         : CN=35b14527-b650-4766-36ac-2158f68f9c3a
   Issuer          : CN=35b14527-b650-4766-36ac-2158f68f9c3a
   Not valid before : Mar  2 06:29:18 2025 GMT
   Not valid after  : Mar  4 06:29:18 2025 GMT
```

## 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: 2021/02/03

### Plugin Output

tcp/8009

```
Subject Name:

Common Name: 35b14527-b650-4766-36ac-2158f68f9c3a

Issuer Name:

Common Name: 35b14527-b650-4766-36ac-2158f68f9c3a

Serial Number: 15 33 6E 86

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Mar 02 06:29:18 2025 GMT
Not Valid After: Mar 04 06:29:18 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 DC 46 ED 4D 3E C9 65 BB E5 B0 5B E6 9D 9F 80 D0 BF 0D 1C
            BC 5E 68 A3 C5 AA 39 D9 98 97 83 83 9D 9F 56 B9 E7 2C 20 1B
            15 4C 57 C3 7E C7 21 8E 6C 2B 4B 61 83 38 5D 49 F1 F2 84 C7
            70 92 77 7B F2 F5 EB A0 6C EC 8E CB D2 3E E5 2B 91 C7 1B 85
            53 4C 75 5D 88 0F 5C 52 06 FA 15 FA 6B 23 29 91 35 40 3D D8
            54 B0 A5 2E F6 E4 3F 92 9B D1 D9 5E A8 8B FB 88 11 C4 4E D9
            8B 72 18 34 4E 82 6E EE F7 B6 5E 4F 7C E5 28 A0 26 A2 9B C0
            EE 2B 23 C4 26 1B 65 CA 3F 25 DE 42 E3 97 BC 32 0A 3C E2 D5
            6C B8 31 5C 51 22 9D DE 0D 3E C0 5A 44 6C 4E F9 75 DA 92 7D
            85 E9 94 C5 EC BB 11 4D 3C 1B 51 48 DB A0 A4 DC 1E 58 D6 1E
            B4 4F 09 E1 5B 91 27 9E C7 0D CA FC 97 93 D6 D0 B7 F8 19 77
```

```
              0E 40 B2 59 20 0C AD 3F 82 A7 CB 70 F8 F0 D7 C9 BB D8 55 C6
              E9 F9 BA D9 66 2A A2 8A B4 F0 62 D6 FB 7A 1F B0 7F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 89 C5 8A F5 5C EA 17 B0 44 68 2E CB 8C 6D 75 76 47 15 7A
              9F 0C 33 BE 17 54 52 2D AA 4A 5E CB 25 57 1B C1 94 40 E8 4A
              9F DE 0B 67 DD 2D 99 73 93 F5 65 05 44 90 00 35 2D 72 ED E6
              75 35 84 67 45 1D 04 CE CF 6F 30 E6 40 D9 75 A7 DA 2A 85 47
              2C 7C 40 7F 9D 3C 4D C8 A0 67 B5 96 7E E6 75 BD 24 32 8C B4
              80 61 5F 84 CA 71 14 CF A4 A0 55 CE DF 3A 0C C8 1C 7E 10 2B
              96 5C 36 04 26 4D E1 40 9F C6 67 43 DA 1A 04 5A 6C 73 63 80
              DB 96 B2 D6 C6 E9 A8 6C F1 BA AD DE B8 A9 73 A7 05 36 87 95
              B0 BE 97 4B 6E FD 99 11 40 F9 34 91 F3 CB 15 AB BF 14 F0 BB
              AA B8 09 3F  [...]
```

## 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: 2021/02/03

Plugin Output

tcp/8443/www

```
Subject Name:

Common Name: 62B38B484108 FA8FCA6E16AD
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Issuer Name:

Common Name: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Serial Number: 68 CD 98 9B 89 19 3F 6C

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 20:37:17 2019 GMT
Not Valid After: May 29 20:37:17 2039 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AA 0A F7 F7 FF 7F 88 2C 01 F5 9F CD C4 02 75 CB 67 85 F3
            6D FE 84 30 02 40 95 1C 13 9D 6F 6C 97 72 59 CA B0 6F CD 96
            A3 F0 ED C3 53 66 ED 06 72 22 4A EB 70 04 D2 77 37 F6 0E 26
            62 BE 82 B5 C9 82 E7 E2 10 5D C7 BF B6 A8 BB 15 C0 E8 CD DB
            46 47 34 9F 0D A6 D2 6C A5 C1 14 CA 8C 34 42 DF 89 6E 89 90
            76 63 6A 95 8D 96 0C 01 B3 3A 3E E1 2F 4F BF 46 C2 39 C9 8A
            E2 F9 A0 0A A6 7D 85 68 7A E6 28 C3 4D 45 C0 5E 7D 8C E0 F2
```

```
            6B 68 90 88 4C F1 0D 2C 53 71 E8 05 B6 4F 42 C0 73 EF 01 73
            80 EF 23 7E 6F FA 52 47 E0 4D 27 78 42 88 12 A0 BE AF 24 DE
            2E 09 F3 F2 2A A7 E6 7F 14 1C 3F 07 AA 2E 9E C7 0A 91 E4 C3
            F3 23 2A 1C BF 46 94 C4 BF F8 E3 10 EC F8 4A 9F 5F 25 A0 AF
            54 0B B6 38 FC 47 F6 9D 12 EB CB BB FF B9 F2 84 87 62 D7 A9
            57 99 25 E5 CB 59 F6 3A EF 69 0B BD C1 C0 1B F8 61
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7E D8 B3 52 05 90 54 CB 7C 6D E4 FF 71 FE BA FE 8F B7 0F
            5C A9 68 DF B5 71 BB 31 00 ED E6 10 6C 5D 84 0A E4 B2 68 2D
            24 24 2A 46 B2 F1 51 73 8F AC F3 50 E7 87 D4 A1 9E 4D F3 2A
            35 F9 A3 20 2B 15 F7 4C 50 E2 66 29 C4 6C 38 10 73 E7 D4 AE
            F1 9E 0F 44 28 CD CB 13 FF C0 34 E1 11 EB CC EB 60 46 F8 EF
            81 4F 12 DD C1 73 F8 D8 19 29 56 F0 76 5C 41 6F 80 90 0A EC
  [...]
```

## 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: 2021/02/03

### Plugin Output

tcp/9000

```
Subject Name:

Common Name: 62B38B484108 FA8FCA6E16AD
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Issuer Name:

Common Name: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Serial Number: 68 CD 98 9B 89 19 3F 6C

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 20:37:17 2019 GMT
Not Valid After: May 29 20:37:17 2039 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AA 0A F7 F7 FF 7F 88 2C 01 F5 9F CD C4 02 75 CB 67 85 F3
            6D FE 84 30 02 40 95 1C 13 9D 6F 6C 97 72 59 CA B0 6F CD 96
            A3 F0 ED C3 53 66 ED 06 72 22 4A EB 70 04 D2 77 37 F6 0E 26
            62 BE 82 B5 C9 82 E7 E2 10 5D C7 BF B6 A8 BB 15 C0 E8 CD DB
            46 47 34 9F 0D A6 D2 6C A5 C1 14 CA 8C 34 42 DF 89 6E 89 90
            76 63 6A 95 8D 96 0C 01 B3 3A 3E E1 2F 4F BF 46 C2 39 C9 8A
            E2 F9 A0 0A A6 7D 85 68 7A E6 28 C3 4D 45 C0 5E 7D 8C E0 F2
```

```
            6B 68 90 88 4C F1 0D 2C 53 71 E8 05 B6 4F 42 C0 73 EF 01 73
            80 EF 23 7E 6F FA 52 47 E0 4D 27 78 42 88 12 A0 BE AF 24 DE
            2E 09 F3 F2 2A A7 E6 7F 14 1C 3F 07 AA 2E 9E C7 0A 91 E4 C3
            F3 23 2A 1C BF 46 94 C4 BF F8 E3 10 EC F8 4A 9F 5F 25 A0 AF
            54 0B B6 38 FC 47 F6 9D 12 EB CB BB FF B9 F2 84 87 62 D7 A9
            57 99 25 E5 CB 59 F6 3A EF 69 0B BD C1 C0 1B F8 61
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7E D8 B3 52 05 90 54 CB 7C 6D E4 FF 71 FE BA FE 8F B7 0F
            5C A9 68 DF B5 71 BB 31 00 ED E6 10 6C 5D 84 0A E4 B2 68 2D
            24 24 2A 46 B2 F1 51 73 8F AC F3 50 E7 87 D4 A1 9E 4D F3 2A
            35 F9 A3 20 2B 15 F7 4C 50 E2 66 29 C4 6C 38 10 73 E7 D4 AE
            F1 9E 0F 44 28 CD CB 13 FF C0 34 E1 11 EB CC EB 60 46 F8 EF
            81 4F 12 DD C1 73 F8 D8 19 29 56 F0 76 5C 41 6F 80 90 0A EC
   [...]
```

## 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: 2021/02/03

### Plugin Output

tcp/10001

```
Subject Name:

Common Name: 62B38B484108 FA8FCA6E16AD
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Issuer Name:

Common Name: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Serial Number: 68 CD 98 9B 89 19 3F 6C

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 20:37:17 2019 GMT
Not Valid After: May 29 20:37:17 2039 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AA 0A F7 F7 FF 7F 88 2C 01 F5 9F CD C4 02 75 CB 67 85 F3
            6D FE 84 30 02 40 95 1C 13 9D 6F 6C 97 72 59 CA B0 6F CD 96
            A3 F0 ED C3 53 66 ED 06 72 22 4A EB 70 04 D2 77 37 F6 0E 26
            62 BE 82 B5 C9 82 E7 E2 10 5D C7 BF B6 A8 BB 15 C0 E8 CD DB
            46 47 34 9F 0D A6 D2 6C A5 C1 14 CA 8C 34 42 DF 89 6E 89 90
            76 63 6A 95 8D 96 0C 01 B3 3A 3E E1 2F 4F BF 46 C2 39 C9 8A
            E2 F9 A0 0A A6 7D 85 68 7A E6 28 C3 4D 45 C0 5E 7D 8C E0 F2
```

```
          6B 68 90 88 4C F1 0D 2C 53 71 E8 05 B6 4F 42 C0 73 EF 01 73
          80 EF 23 7E 6F FA 52 47 E0 4D 27 78 42 88 12 A0 BE AF 24 DE
          2E 09 F3 F2 2A A7 E6 7F 14 1C 3F 07 AA 2E 9E C7 0A 91 E4 C3
          F3 23 2A 1C BF 46 94 C4 BF F8 E3 10 EC F8 4A 9F 5F 25 A0 AF
          54 0B B6 38 FC 47 F6 9D 12 EB CB BB FF B9 F2 84 87 62 D7 A9
          57 99 25 E5 CB 59 F6 3A EF 69 0B BD C1 C0 1B F8 61
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7E D8 B3 52 05 90 54 CB 7C 6D E4 FF 71 FE BA FE 8F B7 0F
          5C A9 68 DF B5 71 BB 31 00 ED E6 10 6C 5D 84 0A E4 B2 68 2D
          24 24 2A 46 B2 F1 51 73 8F AC F3 50 E7 87 D4 A1 9E 4D F3 2A
          35 F9 A3 20 2B 15 F7 4C 50 E2 66 29 C4 6C 38 10 73 E7 D4 AE
          F1 9E 0F 44 28 CD CB 13 FF C0 34 E1 11 EB CC EB 60 46 F8 EF
          81 4F 12 DD C1 73 F8 D8 19 29 56 F0 76 5C 41 6F 80 90 0A EC
  [...]
```

## 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: 2021/02/03

### Plugin Output

tcp/10101

```
Subject Name:

Common Name: 62B38B484108 FA8FCA6E16AD
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Issuer Name:

Common Name: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization Unit: 511D37B1CED91711C81558CA0AA69AC54885805395166888C6CE80368A8117C0
Organization: Lenovo

Serial Number: 68 CD 98 9B 89 19 3F 6C

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: May 29 20:37:17 2019 GMT
Not Valid After: May 29 20:37:17 2039 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AA 0A F7 F7 FF 7F 88 2C 01 F5 9F CD C4 02 75 CB 67 85 F3
            6D FE 84 30 02 40 95 1C 13 9D 6F 6C 97 72 59 CA B0 6F CD 96
            A3 F0 ED C3 53 66 ED 06 72 22 4A EB 70 04 D2 77 37 F6 0E 26
            62 BE 82 B5 C9 82 E7 E2 10 5D C7 BF B6 A8 BB 15 C0 E8 CD DB
            46 47 34 9F 0D A6 D2 6C A5 C1 14 CA 8C 34 42 DF 89 6E 89 90
            76 63 6A 95 8D 96 0C 01 B3 3A 3E E1 2F 4F BF 46 C2 39 C9 8A
            E2 F9 A0 0A A6 7D 85 68 7A E6 28 C3 4D 45 C0 5E 7D 8C E0 F2
```

```
            6B 68 90 88 4C F1 0D 2C 53 71 E8 05 B6 4F 42 C0 73 EF 01 73
            80 EF 23 7E 6F FA 52 47 E0 4D 27 78 42 88 12 A0 BE AF 24 DE
            2E 09 F3 F2 2A A7 E6 7F 14 1C 3F 07 AA 2E 9E C7 0A 91 E4 C3
            F3 23 2A 1C BF 46 94 C4 BF F8 E3 10 EC F8 4A 9F 5F 25 A0 AF
            54 0B B6 38 FC 47 F6 9D 12 EB CB BB FF B9 F2 84 87 62 D7 A9
            57 99 25 E5 CB 59 F6 3A EF 69 0B BD C1 C0 1B F8 61
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 7E D8 B3 52 05 90 54 CB 7C 6D E4 FF 71 FE BA FE 8F B7 0F
            5C A9 68 DF B5 71 BB 31 00 ED E6 10 6C 5D 84 0A E4 B2 68 2D
            24 24 2A 46 B2 F1 51 73 8F AC F3 50 E7 87 D4 A1 9E 4D F3 2A
            35 F9 A3 20 2B 15 F7 4C 50 E2 66 29 C4 6C 38 10 73 E7 D4 AE
            F1 9E 0F 44 28 CD CB 13 FF C0 34 E1 11 EB CC EB 60 46 F8 EF
            81 4F 12 DD C1 73 F8 D8 19 29 56 F0 76 5C 41 6F 80 90 0A EC
  [...]
```

## 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: 2021/02/03

### Plugin Output

tcp/8009

```
  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
     --------------------      ----------  ---       ----    --------------------  ---
     ECDHE-RSA-AES128-SHA      0xC0, 0x13  ECDH      RSA     AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA      0xC0, 0x14  ECDH      RSA     AES-CBC(256)
  SHA1
```

```
    AES128-SHA                     0x00, 0x2F      RSA         RSA        AES-CBC(128)
  SHA1
    AES256-SHA                     0x00, 0x35      RSA         RSA        AES-CBC(256)
  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}
```

## 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: 2021/02/03

### Plugin Output

tcp/8443/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

 The fields above are :

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

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

### 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: 2021/02/03

### Plugin Output

tcp/9000

```
  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

  The fields above are :

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

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

**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: 2021/02/03

## Plugin Output

tcp/10001

```
 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

 The fields above are :

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

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

## 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: 2021/02/03

### Plugin Output

tcp/10101

```
 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

 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/man1.0.2/man1/ciphers.html

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/8009

```
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
  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
    --------------------        ----------    ---        ----      --------------------   ---
    ECDHE-RSA-AES128-SHA256     0xC0, 0x2F    ECDH       RSA       AES-GCM(128)
SHA256
    ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8    ECDH       RSA       ChaCha20-Poly1305(256)
SHA256
    RSA-AES128-SHA256           0x00, 0x9C    RSA        RSA       AES-GCM(128)
SHA256
    ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH       RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH       RSA       AES-CBC(256)
SHA1
    AES128-SHA                  0x00, 0x2F    RSA        RSA       AES-CBC(128)
SHA1
    AES256-SHA                  0x00, 0x35    RSA        RSA       AES-CBC(256)
SHA1


SSL Version  [...]
```

## 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

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/8443/www

```
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
    --------------------         ----------    ---       ----     --------------------     ---
    ECDHE-RSA-AES128-SHA256      0xC0, 0x2F    ECDH      RSA      AES-GCM(128)
  SHA256
    ECDHE-RSA-CHACHA20-POLY1305  0xCC, 0xA8    ECDH      RSA      ChaCha20-Poly1305(256)
  SHA256
    ECDHE-RSA-AES128-SHA         0xC0, 0x13    ECDH      RSA      AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA         0xC0, 0x14    ECDH      RSA      AES-CBC(256)
  SHA1


SSL Version : TLSv11
  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


SSL Version : TLSv1
  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

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/man1.0.2/man1/ciphers.html

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/9000

```
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
    --------------------        ----------    ---     ----    --------------------  ---
    ECDHE-RSA-AES128-SHA256     0xC0, 0x2F    ECDH    RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-CHACHA20-POLY1305 0xCC, 0xA8    ECDH    RSA     ChaCha20-Poly1305(256)
  SHA256
    ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH    RSA     AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH    RSA     AES-CBC(256)
  SHA1


SSL Version : TLSv11
  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


SSL Version : TLSv1
  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

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/man1.0.2/man1/ciphers.html

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/10001

```
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
    --------------------         ----------   ---       ----    --------------------    ---
    ECDHE-RSA-AES128-SHA256      0xC0, 0x2F   ECDH      RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-CHACHA20-POLY1305  0xCC, 0xA8   ECDH      RSA     ChaCha20-Poly1305(256)
  SHA256
    ECDHE-RSA-AES128-SHA         0xC0, 0x13   ECDH      RSA     AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA         0xC0, 0x14   ECDH      RSA     AES-CBC(256)
  SHA1


SSL Version : TLSv11
  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


SSL Version : TLSv1
  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

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/man1.0.2/man1/ciphers.html

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2006/06/05, Modified: 2024/09/11

### Plugin Output

tcp/10101

```
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
    --------------------          ----------    ---        ----    --------------------    ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F    ECDH       RSA     AES-GCM(128)
  SHA256
    ECDHE-RSA-CHACHA20-POLY1305   0xCC, 0xA8    ECDH       RSA     ChaCha20-Poly1305(256)
  SHA256
    ECDHE-RSA-AES128-SHA          0xC0, 0x13    ECDH       RSA     AES-CBC(128)
  SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14    ECDH       RSA     AES-CBC(256)
  SHA1


SSL Version : TLSv11
  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


SSL Version : TLSv1
  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

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: 2021/03/09

### Plugin Output

tcp/8009

```
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-CHACHA20-POLY1305 0xCC, 0xA8     ECDH       RSA      ChaCha20-Poly1305(256)
SHA256
    ECDHE-RSA-AES128-SHA        0xC0, 0x13     ECDH       RSA      AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14     ECDH       RSA      AES-CBC(256)
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

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/8443/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-CHACHA20-POLY1305  0xCC, 0xA8 ECDH      RSA      ChaCha20-Poly1305(256)
  SHA256
     ECDHE-RSA-AES128-SHA       0xC0, 0x13   ECDH      RSA      AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA       0xC0, 0x14   ECDH      RSA      AES-CBC(256)
  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

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/9000

```
 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-CHACHA20-POLY1305 0xCC, 0xA8    ECDH      RSA     ChaCha20-Poly1305(256)
 SHA256
    ECDHE-RSA-AES128-SHA        0xC0, 0x13    ECDH      RSA     AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14    ECDH      RSA     AES-CBC(256)
 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

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/10001

```
  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-CHACHA20-POLY1305   0xCC, 0xA8    ECDH        RSA     ChaCha20-Poly1305(256)
  SHA256
     ECDHE-RSA-AES128-SHA          0xC0, 0x13    ECDH        RSA     AES-CBC(128)
  SHA1
     ECDHE-RSA-AES256-SHA          0xC0, 0x14    ECDH        RSA     AES-CBC(256)
  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

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/10101

```
  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-CHACHA20-POLY1305 0xCC, 0xA8   ECDH        RSA     ChaCha20-Poly1305(256)
    SHA256
      ECDHE-RSA-AES128-SHA        0xC0, 0x13   ECDH        RSA     AES-CBC(128)
    SHA1
      ECDHE-RSA-AES256-SHA        0xC0, 0x14   ECDH        RSA     AES-CBC(256)
    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}
```

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

### Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

### Plugin Output

tcp/8009

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
    ECDHE-RSA-AES128-SHA       0xC0, 0x13    ECDH       RSA       AES-CBC(128)
SHA1
    ECDHE-RSA-AES256-SHA       0xC0, 0x14    ECDH       RSA       AES-CBC(256)
SHA1
    AES128-SHA                 0x00, 0x2F    RSA        RSA       AES-CBC(128)
SHA1
    AES256-SHA                 0x00, 0x35    RSA        RSA       AES-CBC(256)
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}

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/8443/www

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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

The fields above are :

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

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/9000

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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

The fields above are :

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

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/10001

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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

The fields above are :

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

## 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 TLS13_AES_128_GCM_SHA256

- 0x13,0x02 TLS13_AES_256_GCM_SHA384

- 0x13,0x03 TLS13_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

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

Plugin Information

Published: 2022/01/20, Modified: 2024/02/12

Plugin Output

tcp/10101

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  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

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: 2024/03/26

Plugin Output

tcp/8009

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

## 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: 2024/03/26

Plugin Output

tcp/8443/www

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

## 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: 2024/03/26

**Plugin Output**

tcp/9000

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

## 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: 2024/03/26

Plugin Output

tcp/10001

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

## 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: 2024/03/26

Plugin Output

tcp/10101

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

## 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

**Plugin Information**

Published: 2007/05/16, Modified: 2023/10/17

**Plugin Output**

tcp/0

## 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

References

XREF                CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/8009

```
  TLSv1.1 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

References

XREF                CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/8443/www

```
  TLSv1.1 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

References

XREF                CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/9000

```
TLSv1.1 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

References

XREF             CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/10001

```
 TLSv1.1 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

References

XREF                CWE:327

Plugin Information

Published: 2019/01/08, Modified: 2023/04/19

Plugin Output

tcp/10101

```
  TLSv1.1 is enabled and the server supports at least one cipher.
```

## 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/8009

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

## 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/8443/www

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

## 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/9000

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

## 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/10001

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

## 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/10101

```
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: 2023/12/13

Plugin Output

tcp/8009

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

## 10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.68.67 to 192.168.68.56 :
192.168.68.67
192.168.68.56

Hop Count: 1
```

## 35711 - Universal Plug and Play (UPnP) Protocol Detection

### Synopsis

The remote device supports UPnP.

### Description

The remote device answered an SSDP M-SEARCH request. Therefore, it supports 'Universal Plug and Play' (UPnP). This protocol provides automatic configuration and device discovery. It is primarily intended for home networks. An attacker could potentially leverage this to discover your network architecture.

### See Also

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

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

http://quimby.gnus.org/internet-drafts/draft-cai-ssdp-v1-03.txt

### Solution

Filter access to this port if desired.

### Risk Factor

None

### Plugin Information

Published: 2009/02/19, Modified: 2018/09/12

### Plugin Output

udp/1900/ssdp

```
 The device responded to an SSDP M-SEARCH request with the following locations :

    http://192.168.68.56:8008/ssdp/device-desc.xml

 And advertises these unique service names :

    uuid:35b14527-b650-4766-36ac-2158f68f9c3a::urn:dial-multiscreen-org:service:dial:1
    uuid:35b14527-b650-4766-36ac-2158f68f9c3a::upnp:rootdevice
    uuid:35b14527-b650-4766-36ac-2158f68f9c3a::urn:dial-multiscreen-org:device:dial:1
```

## 40405 - Web Server Detection (HTTP/1.1)

Synopsis

A web server is running on this port.

Description

The web server on this port responds to HTTP/1.1 requests and appears to ignore HTTP/1.0 requests, which is unusual.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2019/11/22

Plugin Output

tcp/8008/www

## 40405 - Web Server Detection (HTTP/1.1)

Synopsis

A web server is running on this port.

Description

The web server on this port responds to HTTP/1.1 requests and appears to ignore HTTP/1.0 requests, which is unusual.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/07/28, Modified: 2019/11/22

Plugin Output

tcp/8443/www

## 35712 - Web Server UPnP Detection

### Synopsis

The remote web server provides UPnP information.

### Description

Nessus was able to extract some information about the UPnP-enabled device by querying this web server. Services may also be reachable through SOAP requests.

### See Also

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

### Solution

Filter incoming traffic to this port if desired.

### Risk Factor

None

### Plugin Information

Published: 2009/02/19, Modified: 2020/06/12

### Plugin Output

tcp/8008/www

```
Here is a summary of http://192.168.68.56:8008/ssdp/device-desc.xml :

deviceType: urn:dial-multiscreen-org:device:dial:1
friendlyName: Master Bedroom clock
manufacturer: LENOVO
modelName: Lenovo Smart Clock
modelName: Lenovo Smart Clock
ServiceID: urn:dial-multiscreen-org:serviceId:dial
serviceType: urn:dial-multiscreen-org:service:dial:1
controlURL: /ssdp/notfound
eventSubURL: /ssdp/notfound
SCPDURL: /ssdp/notfound
```