



Software scan

Report generated by Tenable Nessus™

Fri, 21 Mar 2025 13:50:17 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

• 10.0.0.1.....	4
• 10.0.0.112.....	69
• 10.0.0.116.....	184
• 10.0.0.129.....	233
• 10.0.0.141.....	314
• 10.0.0.175.....	408
• 10.0.0.176.....	436
• 10.0.0.189.....	442
• 10.0.0.220.....	452
• 10.0.0.237.....	458
• 10.0.0.240.....	464
• 10.0.0.245.....	475

Vulnerabilities by Host

10.0.0.1



Scan Information

Start time: Fri Mar 21 13:08:56 2025

End time: Fri Mar 21 13:32:08 2025

Host Information

IP: 10.0.0.1

MAC Address: AC:4C:A5:FB:C8:4A

OS: Nutanix

Vulnerabilities

50686 - IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.

Description

The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution

On Linux, you can disable IP forwarding by doing :

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

On Mac OS X, you can disable IP forwarding by executing the command :

```
sysctl -w net.inet.ip.forwarding=0
```

For other systems, check with your vendor.

Risk Factor

Medium

CVSS v3.0 Base Score

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

VPR Score

4.0

EPSS Score

0.0596

CVSS v2.0 Base Score

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

References

CVE CVE-1999-0511

Plugin Information

Published: 2010/11/23, Modified: 2023/10/17

Plugin Output

tcp/0

```
IP forwarding appears to be enabled on the remote host.
```

```
Detected local MAC Address      : 000c29aa8ff9
Response from local MAC Address : 000c29aa8ff9
```

```
Detected Gateway MAC Address    : ac4ca5fbc84a
Response from Gateway MAC Address : ac4ca5fbc84a
```

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>

<https://security.paloaltonetworks.com/PAN-SA-2020-0007>

Solution

Upgrade to JQuery version 3.5.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

5.7

EPSS Score

0.0914

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025
XREF	CISA-KNOWN-EXPLOITED:2025/02/13

Plugin Information

Published: 2020/05/28, Modified: 2025/01/24

Plugin Output

tcp/80/www

```
URL           : http://10.0.0.1/cmn/js/lib/jquery-3.4.1.js
Installed version : 3.4.1
Fixed version  : 3.5.0
```

136929 - JQuery 1.2 < 3.5.0 Multiple XSS

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>

<https://security.paloaltonetworks.com/PAN-SA-2020-0007>

Solution

Upgrade to JQuery version 3.5.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:F/RL:O/RC:C)

VPR Score

5.7

EPSS Score

0.0914

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025
XREF	CISA-KNOWN-EXPLOITED:2025/02/13

Plugin Information

Published: 2020/05/28, Modified: 2025/01/24

Plugin Output

tcp/443/www

```
URL           : https://10.0.0.1/cmn/js/lib/jquery-3.4.1.js
Installed version : 3.4.1
Fixed version   : 3.5.0
```

10663 - DHCP Server Detection

Synopsis

The remote DHCP server may expose information about the associated network.

Description

This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.

Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.

It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.

Solution

Apply filtering to keep this information off the network and remove any options that are not in use.

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2001/05/05, Modified: 2019/03/06

Plugin Output

udp/67

```
Nessus gathered the following information from the remote DHCP server :
```

```
Master DHCP server of this network : 10.0.0.1
IP address the DHCP server would attribute us : 10.0.0.141
DHCP server(s) identifier : 10.0.0.1
Netmask : 255.255.255.0
Broadcast address : 10.0.0.255
Router : 10.0.0.1
Domain name server(s) : 64.71.255.204 , 64.71.255.198
```

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

2.9

EPSS Score

0.0045

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: 2025/03/13

Plugin Output

tcp/0

```
Following application CPE matched on the remote system :
```

```
cpe:/a:jquery:jquery:3.4.1 -> jQuery
```

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

72779 - DNS Server Version Detection

Synopsis

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

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030

XREF IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

Plugin Output

tcp/53/dns

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

```
dnsmasq-2.83
```


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: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose  
Confidence level : 70
```

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 :
```

```
AC:4C:A5:FB:C8:4A : Vantiva USA LLC
```

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:  
- AC:4C:A5:FB:C8:4A
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :  
Xfinity Broadband Router Server
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :  
Xfinity Broadband Router Server
```

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 : no

Options allowed : OPTIONS, GET, HEAD, POST

Headers :

Content-type: text/html

X-robots-tag: noindex,nofollow

X-Frame-Options: deny

X-XSS-Protection: 1; mode=block

X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=15768000; includeSubdomains

Pragma: no-cache

Cache-Control: no-store, no-cache, must-revalidate

Content-Security-Policy: default-src 'self' ; style-src 'self' ; frame-src 'self' ; font-src

'self' ; form-action 'self' ; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self';

connect-src 'self'; object-src 'none'; media-src 'none'; script-nonce 'none'; plugin-types 'none';

reflected-xss 'none'; report-uri 'none';

Content-Length: 8652

Connection: close

Date: Sun, 04 Jan 1970 19:41:43 GMT

Server: Xfinity Broadband Router Server

Response Body :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
<title>Rogers</title>
<!--CSS-->
<link rel="stylesheet" type="text/css" media="screen" href="/cmn/css/common-min.css" />
<!--[if IE 6]>
<link rel="stylesheet" type="text/css" href="/cmn/css/ie6-min.css" />
<![endif]-->
<!--[if IE 7]>
<link rel="stylesheet" type="text/css" href="/cmn/css/ie7-min.css" />
<![endif]-->
<link rel="stylesheet" type="text/css" media="print" href="/cmn/css/print.css" />
<link rel="stylesheet" type="text/css" media="screen" href="/cmn/css/lib/jquery.radioswitch.css" />
<link rel="stylesheet" type="text/css" media="screen" href="/cmn/css/lib/progressBar.css" />
<!--Character Encoding-->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="robots" content="noindex,nofollow">
<script type="text/javascript" src="/cmn/js/lib/jquery-3.4.1.js"></script>
<script type="text/javascript" src="/cmn/js/lib/jquery-migrate-1. [...]
```

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 : no
```

```
Options allowed : OPTIONS, GET, HEAD, POST
```

```
Headers :
```

```
Content-type: text/html
```

```
X-robots-tag: noindex,nofollow
```

```
X-Frame-Options: deny
```

```
X-XSS-Protection: 1; mode=block
```

```
X-Content-Type-Options: nosniff
```

```
Strict-Transport-Security: max-age=15768000; includeSubdomains
```

```
Pragma: no-cache
```

```
Cache-Control: no-store, no-cache, must-revalidate
```

```
Content-Security-Policy: default-src 'self' ; style-src 'self' ; frame-src 'self' ; font-src
```

```
'self' ; form-action 'self' ; script-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self';
```

```
connect-src 'self'; object-src 'none'; media-src 'none'; script-nonce 'none'; plugin-types 'none';
```

```
reflected-xss 'none'; report-uri 'none';
```

```
Content-Length: 8652
```

```
Connection: close
```

```
Date: Sun, 04 Jan 1970 19:41:55 GMT
```

```
Server: Xfinity Broadband Router Server
```


Response Body :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">

<head>
<title>Rogers</title>
<!--CSS-->
<link rel="stylesheet" type="text/css" media="screen" href="./cmn/css/common-min.css" />
<!--[if IE 6]>
<link rel="stylesheet" type="text/css" href="./cmn/css/ie6-min.css" />
<![endif]-->
<!--[if IE 7]>
<link rel="stylesheet" type="text/css" href="./cmn/css/ie7-min.css" />
<![endif]-->
<link rel="stylesheet" type="text/css" media="print" href="./cmn/css/print.css" />
<link rel="stylesheet" type="text/css" media="screen" href="./cmn/css/lib/jquery.radioswitch.css" />
<link rel="stylesheet" type="text/css" media="screen" href="./cmn/css/lib/progressBar.css" />
<!--Character Encoding-->
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
    <meta name="robots" content="noindex, nofollow">
<script type="text/javascript" src="./cmn/js/lib/jquery-3.4.1.js"></script>
<script type="text/javascript" src="./cmn/js/lib/jquery-migrate-1 [...]
```

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/49152/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 :

SERVER: Linux/5.4.201-prod-23.2-231009, UPnP/1.0, Portable SDK for UPnP devices/1.6.22

CONNECTION: close

CONTENT-LENGTH: 48

CONTENT-TYPE: text/html

Response Body :

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

<https://jquery.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/80/www

```
URL      : http://10.0.0.1/cmn/js/lib/jquery-3.4.1.js
Version  : 3.4.1
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

<https://jquery.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2024/02/08

Plugin Output

tcp/443/www

```
URL      : https://10.0.0.1/cmn/js/lib/jquery-3.4.1.js
Version  : 3.4.1
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

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
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

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
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

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
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1883

```
Port 1883/tcp was found to be open
```


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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 178.626 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:09 EDT (UTC -04:00)
Scan duration : 1380 sec
Scan for malware : no
```

42823 - Non-compliant Strict Transport Security (STS)

Synopsis

The remote web server implements Strict Transport Security incorrectly.

Description

The remote web server implements Strict Transport Security. However, it does not respect all the requirements of the STS draft standard.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2014/09/19

Plugin Output

tcp/80/www

```
The Strict-Transport-Security header must not be sent over an
unencrypted channel.
```

42823 - Non-compliant Strict Transport Security (STS)

Synopsis

The remote web server implements Strict Transport Security incorrectly.

Description

The remote web server implements Strict Transport Security. However, it does not respect all the requirements of the STS draft standard.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/11/16, Modified: 2014/09/19

Plugin Output

tcp/443/www

The response from the web server listening on port 80 :

- does not contain a Status-Code of 301.
- does not contain a Location header field.

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Arista EOS
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Cisco CGM4331COM DNI1903A0SP
Confidence level : 30
Method : UPnP
Type : wireless-access-point
Fingerprint : unknown

Remote operating system : Nutanix
Confidence level : 70
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:

P1:B10113:F0x12:W64240:00204ffff:M1460:
P2:B10113:F0x12:W65160:00204ffff0402080affffff4445414401030307:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191003_7_p=80

Following fingerprints could not be used to determine OS :

HTTP!:SERVER: Linux/5.4.201-prod-23.2-231009, UPnP/1.0, Portable SDK for UPnP devices/1.6.22

```
SSLcert:!:i/CN:COMODO RSA Organization Validation Secure Server CAi/O:COMODO CA Limiteds/  
CN:myrouter.ios/O:Comcast Corporation  
1f2152ee6f22aadf6fac9dbde4209c48823d2e6f
```

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 : Nutanix
Confidence level : 70
Method : SinFP
```

```
The remote host is running Nutanix
```

66334 - Patch Report

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/03/11

Plugin Output

tcp/0

```
. You need to take the following action :  
[ JQuery 1.2 < 3.5.0 Multiple XSS (136929) ]  
+ Action to take : Upgrade to JQuery version 3.5.0 or later.
```


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 TLSv1.3/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Country: US
State/Province: Pennsylvania
Organization: Comcast Corporation
Common Name: myrouter.io

Issuer Name:

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

Serial Number: 00 D8 17 65 94 24 2F 07 6C 75 B0 76 F3 14 81 40 3F

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 15 00:00:00 2024 GMT
Not Valid After: Jul 15 23:59:59 2025 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AF C1 E8 8C C1 35 8E ED A9 D1 D7 14 66 90 CE EC 4A 38 34
            BD 80 90 11 03 A5 2C 47 23 5A 62 4E 3E 14 58 17 B8 57 38 DE
            3D 9B AD 6B A9 97 22 81 74 92 7A ED 42 07 32 0A 1E 3A 12 4E
            C4 CB EA 35 42 B3 08 B0 8D 3B 34 FC AF 82 0D 7C 02 98 33 37
```

```
82 2A 87 F9 B5 24 38 0F 3C 70 50 FB 6E E3 99 24 EA 4F 3E 2A
4B 7E 63 3D B7 D1 B5 BD D7 F2 51 CD 98 47 D3 76 E8 6C 17 88
E6 93 60 13 B7 40 D1 E4 9B 3F 42 F2 03 35 87 C7 67 91 62 85
AF 4D 55 C7 9F 54 46 A9 88 C2 B8 42 F2 F9 B0 C4 EB D9 37 0D
64 41 4A DE 9D 3F E1 48 71 14 3A 64 EC 63 1F 2B 6A 75 E0 A4
71 2C 0D ED 7E F2 A1 58 77 6E 58 1B 8B C1 11 C3 23 09 0D CA
14 9A 15 30 EE 59 A3 23 AC 10 8C 2B B8 79 D3 7A FE 89 AA BE
97 B6 84 0B 16 AD 95 3B CD E1 BB F2 F2 20 3F 21 16 E6 78 49
44 EC D3 89 96 A7 85 25 8F 5B 26 AD E4 60 61 BB E3
```

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 5A 1C C0 3E 5C EC 4F DF 34 08 8A 3C 7E F5 05 79 B6 D2 E4
29 B7 84 5D 97 94 36 49 C9 15 3C A2 88 5D 22 D5 09 B9 A9 64
D2 1C 0E 4E DC 91 F7 73 BE 45 C6 88 71 58 F4 2F 7F 88 4D AB
9C 93 10 E5 0C C3 4F 89 67 07 CF 7A AB 2B 1E 9B 0E 7B 7E BF
5F 9D 66 82 D1 D9 64 DE 19 EB 2C 1F 2F 80 01 33 74 EF 8C 9A
19 EF 74 22 1A 40 53 3E AC 43 71 0B FD 63 2A 5D AA C2 AE F6
7E F0 E1 EF E6 DF 19 4E AE [...]

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

Synopsis

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

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities as listed in Tenable Community Knowledge Article 000001752. That is what differentiates this plugin from plugin 35291, which will fire on any certificate, not just known certificate authority root certificates.

Known certificate authority root certificates are inherently trusted and so any potential issues with the signature, including it being signed using a weak hashing algorithm, are not considered security issues.

See Also

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

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

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

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

None

References

BID	11849
BID	33065
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2022/10/12

Plugin Output

tcp/443/www

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

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

Signature Algorithm : SHA-1 With RSA Encryption

Valid From : Jan 01 00:00:00 2004 GMT

Valid To : Dec 31 23:59:59 2028 GMT

Raw PEM certificate :

-----BEGIN CERTIFICATE-----

```
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEhMBkGA1UECAwSR3JlYXRlcjBNYW5jaGVzdGVyMRAwDgYDVQQHDHDA
+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pgy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/
vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/
VruPsUK6+3qsZWY19zjNoFmag4qMsXeDZRRome9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8X1KdH5kBjHYpy
+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIZ6W8Qfs4q8p74K1f9AwPLQwDgYDVR0PAQH/
BAQDAgEGMA8GA1UdEwEB/
wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2Nybc5jb21vZG9jYS5jb20vQUFBQ2VydG1maWNhdGVtZXJ2aWNlcy5jcmwwNqA0oDKGMGH
+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rC17r
+8dFRBv/38ErjHT1r0iWAFf2C3BURz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9l1lawg6nCpnBBYurDC/
zXDrPbDdVCYfeU0BsW0/8tqtlbgT2G9w84FoVxp7Z8VlIMCF1A2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgc
+ev+to5lbyrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgrQAEFQ8TmDn5XpNpaYbg==
-----END CERTIFICATE-----
```

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/443/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
-----	-----	---	----	-----	---
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)	
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)	
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)	

AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA256 SHA256	0x00, 0x6B	DH	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)

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?e17ffcd>

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

```
SSL Version : TLSv13
```

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

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

```
SSL Version : TLSv12
```

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

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

DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)
DHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)
ECDHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)
RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)
RSA-AES256-SHA384 SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA [...]	

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/443/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
-----	-----	---	----	-----	---
DHE-RSA-AES128-SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
SHA256					
DHE-RSA-AES256-SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
SHA384					
DHE-RSA-CHACHA20-POLY1305	0xCC, 0xAA	DH	RSA	ChaCha20-Poly1305(256)	
SHA256					
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
SHA256					
ECDHE-RSA-AES256-SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	
SHA384					

ECDHE-RSA-CHACHA20-POLY1305 SHA256	0xCC, 0xA8	ECDH	RSA	ChaCha20-Poly1305(256)
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)
DHE-RSA-AES256-SHA256 SHA256	0x00, 0x6B	DH	RSA	AES-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)

The fields above are :

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443/www

The following root Certification Authority certificate was found :

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

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 recommended cipher suites.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/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
-----	-----	----	----	-----	----
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x9E	DH	RSA	AES-GCM(128)	
DHE-RSA-AES256-SHA384 SHA384	0x00, 0x9F	DH	RSA	AES-GCM(256)	
RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	
RSA-AES256-SHA384 SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
DHE-RSA-AES128-SHA SHA1	0x00, 0x33	DH	RSA	AES-CBC(128)	
DHE-RSA-AES256-SHA SHA1	0x00, 0x39	DH	RSA	AES-CBC(256)	
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)	
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)	
DHE-RSA-AES128-SHA256 SHA256	0x00, 0x67	DH	RSA	AES-CBC(128)	
DHE-RSA-AES256-SHA256 SHA256	0x00, 0x6B	DH	RSA	AES-CBC(256)	
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)	
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	

The fields above are :

{Tenable ciphername [...]}

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.
```


42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/80/www

The STS header line is :

Strict-Transport-Security: max-age=15768000; includeSubdomains

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

The STS header line is :

Strict-Transport-Security: max-age=15768000; includeSubdomains

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

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/html/rfc7301>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1
```

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/443/www

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/443/www

```
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 10.0.0.141 to 10.0.0.1 :  
10.0.0.141  
10.0.0.1  
  
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://10.0.0.1:49152/IGDdevicedesc_brlan0.xml`

And advertises these unique service names :

```
uuid:ebf5a0a0-1dd1-11b2-a90f-ac4ca5fbc84a::upnp:rootdevice
uuid:ebf5a0a0-1dd1-11b2-a90f-ac4ca5fbc84a::urn:schemas-upnp-org:device:InternetGatewayDevice:1
uuid:ebf5a0a0-1dd1-11b2-a90f-ac4ca5fbc84a::urn:schemas-upnp-org:service:Layer3Forwarding:1
uuid:ebf5a0a0-1dd1-11b2-a92f-ac4ca5fbc84a::urn:schemas-upnp-org:device:WANDevice:1
uuid:ebf5a0a0-1dd1-11b2-a92f-ac4ca5fbc84a::urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
uuid:ebf5a0a0-1dd1-11b2-a93f-ac4ca5fbc84a::urn:schemas-upnp-org:device:WANConnectionDevice:1
uuid:ebf5a0a0-1dd1-11b2-a93f-ac4ca5fbc84a::urn:schemas-upnp-org:service:WANIPConnection:1
```


10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

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

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/443/www

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

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

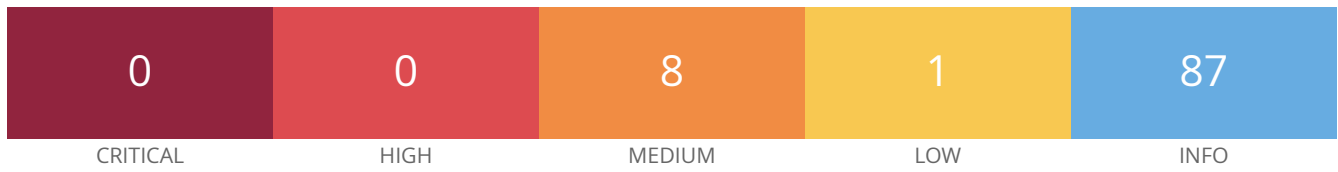
tcp/49152/www

Here is a summary of `http://10.0.0.1:49152/IGDdevicedesc_brlan0.xml` :

```
deviceType: urn:schemas-upnp-org:device:InternetGatewayDevice:1
friendlyName: CGM4331COM
manufacturer: Cisco
manufacturerURL: http://www.cisco.com/
modelName: CGM4331COM
modelDescription: CGM4331COM
modelName: CGM4331COM
modelNumber: CGM4331COM
modelURL: http://www.cisco.com
serialNumber:
ServiceID: urn:upnp-org:serviceId:L3Forwarding1
serviceType: urn:schemas-upnp-org:service:Layer3Forwarding:1
controlURL: /upnp/control/Layer3Forwarding
eventSubURL: /upnp/event/Layer3Forwarding
SCPDURL: /Layer3ForwardingSCPD.xml
ServiceID: urn:upnp-org:serviceId:WANCommonIFC1
serviceType: urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
controlURL: /upnp/control/WANCommonInterfaceConfig0
eventSubURL: /upnp/event/WANCommonInterfaceConfig0
SCPDURL: /WANCommonInterfaceConfigSCPD.xml
ServiceID: urn:upnp-org:serviceId:WANIPConn1
```

```
serviceType: urn:schemas-upnp-org:service:WANIPConnection:1
controlURL: /upnp/control/WANIPConnection0
eventSubURL: /upnp/event/WANIPConnection0
SCPDURL: /WANIPConnectionServiceSCPD.xml
```

10.0.0.112



Scan Information

Start time: Fri Mar 21 13:09:31 2025
End time: Fri Mar 21 13:16:57 2025

Host Information

Netbios Name: RIS430-TARGET
IP: 10.0.0.112
MAC Address: 00:0C:29:AF:11:9D
OS: Linux Kernel 2.6

Vulnerabilities

12217 - DNS Server Cache Snooping Remote Information Disclosure

Synopsis

The remote DNS server is vulnerable to cache snooping attacks.

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

See Also

http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Solution

Contact the vendor of the DNS software for a fix.

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)

CVSS v2.0 Base Score

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

Plugin Information

Published: 2004/04/27, Modified: 2020/04/07

Plugin Output

udp/53/dns

```
Nessus sent a non-recursive query for example.com  
and received 6 answers :
```

```
23.215.0.138  
96.7.128.175  
23.192.228.80  
23.215.0.136  
96.7.128.198  
23.192.228.84
```

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

<http://www.nessus.org/u?df39b8b3>

<http://technet.microsoft.com/en-us/library/cc731957.aspx>

<http://www.nessus.org/u?74b80723>

<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>

<http://www.nessus.org/u?a3cac4ea>

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further 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:N/I:L/A:N)

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

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

Solution

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

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

4.4

EPSS Score

0.027

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

BID 28482
CVE CVE-2007-1858

Plugin Information

Published: 2008/03/28, Modified: 2023/10/27

Plugin Output

tcp/25/smtp

The following is a list of SSL anonymous ciphers supported by the remote TCP server :

High Strength Ciphers (>= 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	----	-----	----
SHA256 DH-AES128-SHA256	0x00, 0xA6	DH	None	AES-GCM(128)	
SHA384 DH-AES256-SHA384	0x00, 0xA7	DH	None	AES-GCM(256)	
SHA1 ADH-AES128-SHA	0x00, 0x34	DH	None	AES-CBC(128)	
SHA1 ADH-AES256-SHA	0x00, 0x3A	DH	None	AES-CBC(256)	
SHA1 ADH-CAMELLIA128-SHA	0x00, 0x46	DH	None	Camellia-CBC(128)	
SHA1 ADH-CAMELLIA256-SHA	0x00, 0x89	DH	None	Camellia-CBC(256)	
SHA1 AECDH-AES128-SHA	0xC0, 0x18	ECDH	None	AES-CBC(128)	
SHA1 AECDH-AES256-SHA	0xC0, 0x19	ECDH	None	AES-CBC(256)	
SHA256 DH-AES128-SHA256	0x00, 0x6C	DH	None	AES-CBC(128)	
SHA256 DH-AES256-SHA256	0x00, 0x6D	DH	None	AES-CBC(256)	
SHA256 DH-CAMELLIA128-SHA256	0x00, 0xBF	DH	None	Camellia-CBC(128)	
SHA256 DH-CAMELLIA256-SHA256	0x00, 0xC5	DH	None	Camellia-CBC(256)	

The fields above are :

{Tenable ciphertype}
{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/25/smtp

```
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=ubuntu
| -Issuer  : CN=ubuntu
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/25/smtp

```
The identities known by Nessus are :
```

```
10.0.0.112
10.0.0.112
```

```
The Common Name in the certificate is :
```

```
ubuntu
```

```
The Subject Alternate Name in the certificate is :
```

```
ubuntu
```

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/25/smtp

```
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=ubuntu
```

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/25/smtp

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/25/smtp

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

2.9

EPSS Score

0.0045

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 second.

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL      : http://10.0.0.112/
Version  : 2.4.99
Source   : Server: Apache/2.4.52 (Ubuntu)
backported : 1
os       : ConvertedUbuntu
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/22/ssh

```
Give Nessus credentials to perform local checks.
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80/www

```
Give Nessus credentials to perform local checks.
```

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: 2025/03/13

Plugin Output

tcp/0

The remote operating system matched the following CPE :

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

Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.4.52 -> Apache Software Foundation Apache HTTP Server

cpe:/a:apache:http_server:2.4.99 -> Apache Software Foundation Apache HTTP Server

cpe:/a:isc:bind:9.18.30-0ubuntu0.22.04.2-ubuntu -> ISC BIND

cpe:/a:isc:bind:9.18.30:0ubuntu0 -> ISC BIND

cpe:/a:openbsd:openssh:8.9 -> OpenBSD OpenSSH

cpe:/a:openbsd:openssh:8.9p1 -> OpenBSD OpenSSH

cpe:/a:squid-cache:squid:5.9 -> squid-cache.org Squid

10028 - DNS Server BIND version Directive Remote Version Detection

Synopsis

It is possible to obtain the version number of the remote DNS server.

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of BIND by using the 'version' directive in the 'options' section in named.conf.

Risk Factor

None

References

XREF IAVT:0001-T-0583

Plugin Information

Published: 1999/10/12, Modified: 2022/10/12

Plugin Output

udp/53/dns

```
Version : 9.18.30-0ubuntu0.22.04.2-Ubuntu
```

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

72779 - DNS Server Version Detection

Synopsis

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

Description

Nessus was able to obtain version information by sending a special TXT record query to the remote host.

Note that this version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030

XREF IAVT:0001-T-0937

Plugin Information

Published: 2014/03/03, Modified: 2024/09/24

Plugin Output

tcp/53/dns

```
DNS server answer for "VERSION.BIND" (over TCP) :
```

```
9.18.30-0ubuntu0.22.04.2-Ubuntu
```

35371 - DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.

Description

It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.

Solution

It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor

None

Plugin Information

Published: 2009/01/15, Modified: 2011/09/14

Plugin Output

udp/53/dns

```
The remote host name is :
```

```
RIS430-Target
```

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: 2025/03/12

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 :
```

```
00:0C:29:AF:11:9D : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:0C:29:AF:11:9D
```


10092 - FTP Server Detection

Synopsis

An FTP server is listening on a remote port.

Description

It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0030

XREF IAVT:0001-T-0943

Plugin Information

Published: 1999/10/12, Modified: 2023/08/17

Plugin Output

tcp/21/ftp

```
The remote FTP banner is :
```

```
220 (vsFTPd 3.0.5)
```

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_\(OTG-CONFIG-006\)](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 the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :  
Apache/2.4.52 (Ubuntu)
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/3128/http_proxy

```
The remote web server type is :  
squid/5.9
```

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 :

Date: Fri, 21 Mar 2025 17:11:39 GMT

Server: Apache/2.4.52 (Ubuntu)

Last-Modified: Mon, 03 Mar 2025 19:58:40 GMT

ETag: "29af-62f7595281f8d"

Accept-Ranges: bytes

Content-Length: 10671

Vary: Accept-Encoding

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

Response Body :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<!--
```

Modified from the Debian original for Ubuntu

Last updated: 2022-03-22

See: <https://launchpad.net/bugs/1966004>

-->

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Apache2 Ubuntu Default Page: It works</title>

<style type="text/css" media="screen">

* {

margin: 0px 0px 0px 0px;

padding: 0px 0px 0px 0px;

}

body, html {

padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Ubuntu, Verdana, sans-serif;

font-size: 11pt;

text-align: center;

}

div.main_page {

position: relative;

display: table;

width: 800px;

margin-bottom: 3px;

margin-left: auto;

margin-right: auto;

padding: 0px 0px 0px 0px;

border-width: 2px;

border-color: #212738;

border-style: solid;

background-color: #FFFFFF;

text-align: center;

}

div.page_header {

height: 180px;

width: 100%;

background-color: #F5F6F7;

}

div.page_header span {

margin: 15px 0px 0px 50px;

font-size: 180%;

font-weight: bold;

}

div.page_header img {

margin: 3px 0px 0px 40px;

border: 0px 0px 0px;

}

div.banner {

padding: 9px 6px 9px 6px;

background-color: #E9510E;

color: #FFFFFF;

font-weight: bold;

font-size: 112%;

text-align: center;

```
position: absolute;  
left: 40%;  
[...]
```


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/3128/http_proxy

```
Response Code : HTTP/1.1 400 Bad Request
```

```
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 :
```

```
    Server: squid/5.9
```

```
    Mime-Version: 1.0
```

```
    Date: Fri, 21 Mar 2025 17:11:39 GMT
```

```
    Content-Type: text/html;charset=utf-8
```

```
    Content-Length: 3510
```

```
    X-Squid-Error: ERR_INVALID_URL 0
```

```
    Vary: Accept-Language
```

```
    Content-Language: en
```

```
    X-Cache: MISS from RIS430-Target
```

```
    X-Cache-Lookup: NONE from RIS430-Target:3128
```

```
    Via: 1.1 RIS430-Target (squid/5.9)
```

```
    Connection: close
```

```
Response Body :
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
```

```

<meta type="copyright" content="Copyright (C) 1996-2020 The Squid Software Foundation and
contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
/*
 * Copyright (C) 1996-2023 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */

/*
  Stylesheet for Squid Error pages
  Adapted from design by Free CSS Templates
  http://www.freecsstemplates.org
  Released for free under a Creative Commons Attribution 2.5 License
 */

/* Page basics */
* {
font-family: verdana, sans-serif;
}

html body {
margin: 0;
padding: 0;
background: #efefef;
font-size: 12px;
color: #1e1e1e;
}

/* Page displayed title area */
#titles {
margin-left: 15px;
padding: 10px;
padding-left: 100px;
background: url('/squid-internal-static/icons/SN.png') no-repeat left;
}

/* initial title */
#titles h1 {
color: #000000;
}
#titles h2 {
color: #000000;
}

/* special event: FTP success page titles */
#titles ftpsuccess {
background-color: #00ff00;
width: 100%;
}

/* Page displayed body content area */
#content {
padding: 10px;
background: #ffffff;
}

/* General text */
p {
[...]
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/03/30, Modified: 2015/01/12

Plugin Output

tcp/445/cifs

The following password policy is defined on the remote host:

```
Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

See Also

<http://technet.microsoft.com/en-us/library/bb418944.aspx>

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information

Published: 2002/02/13, Modified: 2024/01/31

Plugin Output

tcp/445/cifs

```
The remote host SID value is : S-1-5-21-16712664-3263013029-3023772533
```

```
The value of 'RestrictAnonymous' setting is : unknown
```

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
Nessus was able to obtain the following information about the host, by  
parsing the SMB2 Protocol's NTLM SSP message:
```

```
Target Name: RIS430-TARGET  
NetBIOS Domain Name: RIS430-TARGET  
NetBIOS Computer Name: RIS430-TARGET  
DNS Domain Name:  
DNS Computer Name: ris430-target  
DNS Tree Name: unknown  
Product Version: 6.1.0
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

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

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

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

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

<https://technet.microsoft.com/en-us/library/bb456988.aspx>

<https://technet.microsoft.com/en-us/library/cc783530.aspx>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/07/25, Modified: 2022/08/11

Plugin Output

tcp/445/cifs

```
Share path : \\RIS430-TARGET\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:      YES
    FILE_GENERIC_WRITE:     YES
    FILE_GENERIC_EXECUTE:   YES

Share path : \\RIS430-TARGET\IPC$
Local path : C:\tmp
Comment : IPC Service (RIS430-Target server (Samba, Ubuntu))
[*] Allow ACE for Everyone (S-1-1-0): 0x001f01ff
    FILE_GENERIC_READ:      YES
    FILE_GENERIC_WRITE:     YES
    FILE_GENERIC_EXECUTE:   YES
```


10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/05/09, Modified: 2022/02/01

Plugin Output

tcp/445/cifs

```
Here are the SMB shares available on the remote host :
```

- print\$
- IPC\$

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :  
SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7
3.0        Windows 8
3.0.2      Windows 8.1
3.1.1      Windows 10

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.1        Windows 10
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : netstat
Port range : default
Ping RTT : 203.679 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/3/21 13:09 EDT (UTC -04:00)
Scan duration : 408 sec
Scan for malware : no
```

64582 - Netstat Connection Information

Synopsis

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

Description

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

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/21/ftp

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/22/ssh

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


14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/25/smtp

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/53/dns

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/53/dns

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/68

```
Port 68/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/80/www

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/123/ntp

```
Port 123/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/137/netbios-ns

```
Port 137/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/138

```
Port 138/udp was found to be open
```


14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/139/smb

```
Port 139/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/546

```
Port 546/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/3128/http_proxy

```
Port 3128/tcp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/5353/mdns

```
Port 5353/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/34074

```
Port 34074/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/37892

```
Port 37892/udp was found to be open
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/57352

```
Port 57352/udp was found to be open
```


14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

udp/58034

```
Port 58034/udp was found to be open
```

10884 - Network Time Protocol (NTP) Server Detection

Synopsis

An NTP server is listening on the remote host.

Description

An NTP server is listening on port 123. If not securely configured, it may provide information about its version, current date, current time, and possibly system information.

See Also

<http://www.ntp.org>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0934

Plugin Information

Published: 2015/03/20, Modified: 2021/02/24

Plugin Output

udp/123/ntp

```
An NTP service has been discovered, listening on port 123.  
  
No sensitive information has been disclosed.  
  
Version : unknown
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Linux Kernel 2.6

Confidence level : 65

Method : SinFP

Type : general-purpose

Fingerprint : SinFP:

P1:B10113:F0x12:W64240:00204ffff:M1460:

P2:B10113:F0x12:W65160:00204ffff0402080afffffff4445414401030307:M1460:

P3:B00000:F0x00:W0:00:M0

P4:191003_7_p=139

Following fingerprints could not be used to determine OS :

SSH:!:SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11

NTP:!:unknown

HTTP:!:Server: Apache/2.4.52 (Ubuntu)

SMTP:!:220 RIS430-Target.phub.net.cable.rogers.com ESMTP Postfix (Ubuntu)

SSLcert:!:i/CN:ubuntus/CN:ubuntu

a379b492c7bb5f3647c7ae74cdd0f3c611f0f536

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

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

SSH:!:SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11
NTP:!:unknown
SinFP:
  P1:B10113:F0x12:W64240:00204ffff:M1460:
  P2:B10113:F0x12:W65160:00204ffff0402080affffff4445414401030307:M1460:
  P3:B00000:F0x00:W0:00:M0
  P4:191003_7_p=139
HTTP:!:Server: Apache/2.4.52 (Ubuntu)

SMTP:!:220 RIS430-Target.phub.net.cable.rogers.com ESMTP Postfix (Ubuntu)
SSLcert:!:i/CN:ubuntu/CN:ubuntu
a379b492c7bb5f3647c7ae74cdd0f3c611f0f536

The remote host is running Linux Kernel 2.6
```

181418 - OpenSSH Detection

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

<https://www.openssh.com/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/03/11

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.9p1
Banner  : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11
```

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/25/smtp

10263 - SMTP Server Detection

Synopsis

An SMTP server is listening on the remote port.

Description

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0932

Plugin Information

Published: 1999/10/12, Modified: 2020/09/22

Plugin Output

tcp/25/smtp

```
Remote SMTP server banner :
```

```
220 RIS430-Target.phub.net.cable.rogers.com ESMTP Postfix (Ubuntu)
```

42088 - SMTP Service STARTTLS Command Support

Synopsis

The remote mail service supports encrypting traffic.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/09, Modified: 2019/03/20

Plugin Output

tcp/25/smtp

```
Here is the SMTP service's SSL certificate that Nessus was able to
collect after sending a 'STARTTLS' command :

----- snip -----
Subject Name:

Common Name: ubuntu

Issuer Name:

Common Name: ubuntu

Serial Number: 01 1B 6C 97 BA 5D 55 F4 06 DD 22 32 9D A5 2C F0 B9 4E 95 FA

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 13 16:53:59 2025 GMT
Not Valid After: Feb 11 16:53:59 2035 GMT
```


Public Key Info:

Algorithm: RSA Encryption

Key Length: 2048 bits

Public Key: 00 AE 07 68 DE BD A5 C5 A4 BE EB 74 24 F4 C0 13 99 BC E6 CB
A9 D5 12 78 F2 C6 B0 95 B4 9B C8 52 E3 23 EE 07 EE 39 46 B5
F1 71 50 9B 7F ED 4D B7 4C 6E 41 AB DF CF AE 4D 1A C6 90 72
20 E7 B3 03 C2 6C C3 51 5C 41 81 8D 69 5E BB E1 81 DD 9A 73
74 2F DF 79 02 97 F1 3A AF D6 E3 12 5F B9 49 BE F7 3A 30 71
77 98 46 D8 70 25 63 F1 61 C1 FC F1 53 35 2F FE 36 88 07 04
72 80 56 C0 7D 3C B5 89 A5 C5 0D 3B 81 6F C7 01 24 12 34 4E
81 CB 2F 84 6F 15 50 FE 17 31 A0 0A E6 7A 59 40 4D 06 6E 2B
9C BA 22 63 DA 8E A5 B3 19 5F 08 A2 F6 9D BC 78 0B 7C 41 15
8F 84 1D B6 27 D2 B5 F0 29 E2 2A 7B 59 1F 8A B6 3E 04 DF A6
A0 44 05 78 37 C4 A7 79 E2 C0 7E A6 08 44 6B 54 76 03 DA 63
8F 7C 8C D1 47 2B EB C7 46 8A 88 19 2C EE 76 DA 86 0C 3A EF
47 D6 DE 6F 0F 98 42 15 F5 64 50 F6 68 D9 2B A0 BD

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 59 15 DB 17 E2 BF A3 7F 2B E0 E9 2B 97 17 61 5A A8 37 07
33 03 DE 91 1F 7D C6 E0 CE AB B9 BE E7 BA 4C 07 A2 EC 9B 0E
E9 2D 7C 57 5A 3D 8F 0A A1 D5 E1 FA 21 A5 99 06 C9 B1 F9 8D
8D 11 A9 00 1E 55 A6 C9 CB 29 98 1E 8E 35 5D 62 B5 6F 15 7B
DE A9 81 5D E6 3D 70 3E F0 08 54 04 CB 4D BB 6A DA 78 4E 2F
2F 8B 15 B7 8B D8 FE C9 B0 56 87 36 D2 61 B2 26 16 A7 36 F5
C7 87 C4 19 1A 81 8F 1E 48 15 5F F8 23 3F 34 75 67 C7 6D 3C [...]

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/22/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
zlib@openssh.com
```

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

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

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

```
ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
```

The server supports the following options for `encryption_algorithms_client_to_server` :

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

The server supports the following options for `mac_algorithms_server_to_client` :

```
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com
```

The server supports the following options for `kex_algorithms` :

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
kex-strict-s-v00@openssh.com
sntrup761x25519-sha512@openssh.com
```

The server supports the following options for `compression_algorithms_client_to_server` :

```
none
zlib@openssh.com
```

The server supports the following options for `encryption_algorithms_server_to_client` :

```
aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com
```

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/22/ssh

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
The remote SSH daemon supports the following versions of the  
SSH protocol :
```

- 1.99
- 2.0

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
hmac-sha1
hmac-sha1-etm@openssh.com
```

```
The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
```

```
hmac-sha1
hmac-sha1-etm@openssh.com
```

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/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11
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/25/smtp

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


45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/25/smtp

```
The host name known by Nessus is :
```

```
ris430-target
```

```
The Common Name in the certificate is :
```

```
ubuntu
```

```
The Subject Alternate Name in the certificate is :
```

```
ubuntu
```

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/25/smtp

```
Subject Name:

Common Name: ubuntu

Issuer Name:

Common Name: ubuntu

Serial Number: 01 1B 6C 97 BA 5D 55 F4 06 DD 22 32 9D A5 2C F0 B9 4E 95 FA

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 13 16:53:59 2025 GMT
Not Valid After: Feb 11 16:53:59 2035 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 AE 07 68 DE BD A5 C5 A4 BE EB 74 24 F4 C0 13 99 BC E6 CB
            A9 D5 12 78 F2 C6 B0 95 B4 9B C8 52 E3 23 EE 07 EE 39 46 B5
            F1 71 50 9B 7F ED 4D B7 4C 6E 41 AB DF CF AE 4D 1A C6 90 72
            20 E7 B3 03 C2 6C C3 51 5C 41 81 8D 69 5E BB E1 81 DD 9A 73
            74 2F DF 79 02 97 F1 3A AF D6 E3 12 5F B9 49 BE F7 3A 30 71
            77 98 46 D8 70 25 63 F1 61 C1 FC F1 53 35 2F FE 36 88 07 04
            72 80 56 C0 7D 3C B5 89 A5 C5 0D 3B 81 6F C7 01 24 12 34 4E
            81 CB 2F 84 6F 15 50 FE 17 31 A0 0A E6 7A 59 40 4D 06 6E 2B
            9C BA 22 63 DA 8E A5 B3 19 5F 08 A2 F6 9D BC 78 0B 7C 41 15
            8F 84 1D B6 27 D2 B5 F0 29 E2 2A 7B 59 1F 8A B6 3E 04 DF A6
            A0 44 05 78 37 C4 A7 79 E2 C0 7E A6 08 44 6B 54 76 03 DA 63
```

```
      8F 7C 8C D1 47 2B EB C7 46 8A 88 19 2C EE 76 DA 86 0C 3A EF
      47 D6 DE 6F 0F 98 42 15 F5 64 50 F6 68 D9 2B A0 BD
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 59 15 DB 17 E2 BF A3 7F 2B E0 E9 2B 97 17 61 5A A8 37 07
          33 03 DE 91 1F 7D C6 E0 CE AB B9 BE E7 BA 4C 07 A2 EC 9B 0E
          E9 2D 7C 57 5A 3D 8F 0A A1 D5 E1 FA 21 A5 99 06 C9 B1 F9 8D
          8D 11 A9 00 1E 55 A6 C9 CB 29 98 1E 8E 35 5D 62 B5 6F 15 7B
          DE A9 81 5D E6 3D 70 3E F0 08 54 04 CB 4D BB 6A DA 78 4E 2F
          2F 8B 15 B7 8B D8 FE C9 B0 56 87 36 D2 61 B2 26 16 A7 36 F5
          C7 87 C4 19 1A 81 8F 1E 48 15 5F F8 23 3F 34 75 67 C7 6D 3C
          1C 87 7B F8 89 FB D9 CE DC 7F 82 47 38 7A B1 70 29 AC 5C C2
          0B 37 E8 61 7A F1 1F 14 83 C6 89 CB B5 8C 3F CC 00 66 22 17
          42 5D 9E 39 2A A1 C2 6D [...]
```

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/25/smtp

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-CAMELLIA-CBC-128
SHA256 | 0xC0, 0x76 | ECDH | RSA | Camellia-CBC(128) | |
| ECDHE-RSA-CAMELLIA-CBC-256
SHA384 | 0xC0, 0x77 | ECDH | RSA | Camellia-CBC(256) | |
| DHE-RSA-AES128-SHA
SHA1 | 0x00, 0x33 | DH | RSA | AES-CBC(128) | |
| DHE-RSA-AES256-SHA
SHA1 | 0x00, 0x39 | DH | RSA | AES-CBC(256) | |
| DHE-RSA-CAMELLIA128-SHA
SHA1 | 0x00, 0x45 | DH | RSA | Camellia-CBC(128) | |

| | | | | | |
|---------------------------------|------------|------|------|-------------------|---|
| DHE-RSA-CAMELLIA256-SHA
SHA1 | 0x00, 0x88 | DH | RSA | Camellia-CBC(256) | |
| ADH-AES128-SHA
SHA1 | 0x00, 0x34 | DH | None | AES-CBC(128) | |
| ADH-AES256-SHA
SHA1 | 0x00, 0x3A | DH | None | AES-CBC(256) | |
| ADH-CAMELLIA128-SHA
SHA1 | 0x00, 0x46 | DH | None | Camellia-CBC(128) | |
| ADH-CAMELLIA256-SHA
SHA1 | 0x00, 0x89 | DH | None | Camellia-CBC(256) | |
| ECDHE-RSA-AES128-SHA
SHA1 | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) | |
| ECDHE-RSA-AES256-SHA
SHA1 | 0xC0, 0x14 | ECDH | RSA | AES-CBC(256) | |
| AECDH-AES128-SHA
SHA1 | 0xC0, 0x18 | ECDH | None | AES-CBC(128) | |
| AECDH-AES256-SHA
SHA1 | 0xC0, 0x19 | ECDH | None | AES-CBC(256) | |
| AES128-SHA
SHA1 | 0x00, 0x2F | RSA | RSA | AES-CBC(128) | |
| AES256-SHA
SHA1 | 0x00, 0x35 | RSA | RSA | AES-CBC(256) | |
| CAMELLIA128-SHA
[...] | 0x00, 0x41 | RSA | RSA | Camellia-CBC(128) | S |

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?e17ffcd>

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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

```
SSL Version : TLSv13
```

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

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

```
SSL Version : TLSv12
```

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

| Name | Code | KEX | Auth | Encryption | MAC |
|--------------------------|------------|-----|------|--------------|-----|
| ----- | ----- | --- | --- | ----- | --- |
| DHE-RSA-AES-128-CCM-AEAD | 0xC0, 0x9E | DH | RSA | AES-CCM(128) | |
| AEAD | | | | | |

| | | | | |
|-------------------------------------|------------|------|------|------------------------|
| DHE-RSA-AES-128-CCM8-AEAD
AEAD | 0xC0, 0xA2 | DH | RSA | AES-CCM8(128) |
| DHE-RSA-AES128-SHA256
SHA256 | 0x00, 0x9E | DH | RSA | AES-GCM(128) |
| DHE-RSA-AES-256-CCM-AEAD
AEAD | 0xC0, 0x9F | DH | RSA | AES-CCM(256) |
| DHE-RSA-AES-256-CCM8-AEAD
AEAD | 0xC0, 0xA3 | DH | RSA | AES-CCM8(256) |
| DHE-RSA-AES256-SHA384
SHA384 | 0x00, 0x9F | DH | RSA | AES-GCM(256) |
| DHE-RSA-CHACHA20-POLY1305
SHA256 | 0xCC, 0xAA | DH | RSA | ChaCha20-Poly1305(256) |
| DH-AES128-SHA256
SHA256 | 0x00, 0xA6 | DH | None | AES-GCM(128) |
| DH-AES256-SHA384
SHA384 | 0x00, 0xA7 | DH | None | AES-GCM(256) |
| ECDHE-RSA-AES128-SHA256
SHA256 | 0xC0, 0x2F | ECDH | RSA | AES-GCM(128) |
| ECDHE-RSA-AES256-SHA384 | 0xC0, 0x30 | ECDH | RSA | [...] |

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/25/smtp

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

High Strength Ciphers (>= 112-bit key)

| Name | Code | KEX | Auth | Encryption | MAC |
|---------------------------|------------|-----|------|---------------|-----|
| ----- | ----- | --- | ---- | ----- | --- |
| DHE-RSA-AES-128-CCM-AEAD | 0xC0, 0x9E | DH | RSA | AES-CCM(128) | |
| AEAD | | | | | |
| DHE-RSA-AES-128-CCM8-AEAD | 0xC0, 0xA2 | DH | RSA | AES-CCM8(128) | |
| AEAD | | | | | |
| DHE-RSA-AES128-SHA256 | 0x00, 0x9E | DH | RSA | AES-GCM(128) | |
| SHA256 | | | | | |
| DHE-RSA-AES-256-CCM-AEAD | 0xC0, 0x9F | DH | RSA | AES-CCM(256) | |
| AEAD | | | | | |
| DHE-RSA-AES-256-CCM8-AEAD | 0xC0, 0xA3 | DH | RSA | AES-CCM8(256) | |
| AEAD | | | | | |

| | | | | |
|---------------------------------------|------------|------|-----|------------------------|
| DHE-RSA-AES256-SHA384
SHA384 | 0x00, 0x9F | DH | RSA | AES-GCM(256) |
| DHE-RSA-CHACHA20-POLY1305
SHA256 | 0xCC, 0xAA | DH | RSA | ChaCha20-Poly1305(256) |
| ECDHE-RSA-AES128-SHA256
SHA256 | 0xC0, 0x2F | ECDH | RSA | AES-GCM(128) |
| ECDHE-RSA-AES256-SHA384
SHA384 | 0xC0, 0x30 | ECDH | RSA | AES-GCM(256) |
| ECDHE-RSA-CAMELLIA-CBC-128
SHA256 | 0xC0, 0x76 | ECDH | RSA | Camellia-CBC(128) |
| ECDHE-RSA-CAMELLIA-CBC-256
SHA384 | 0xC0, 0x77 | ECDH | RSA | Camellia-CBC(256) |
| ECDHE-RSA-CHACHA20-POLY1305
SHA256 | 0xCC, 0xA8 | ECDH | RSA | ChaCha20-Poly1305(256) |
| DHE-RSA-AES128-SHA
SHA1 | 0x00, 0x33 | DH | RSA | AES-CBC(128) |
| DHE-RSA-AES256-SHA
SHA1 | 0x00, 0x39 | DH | RSA | AES-CBC(256) |
| DHE-RSA-CAMELLIA128-SHA
SHA1 | 0x00, 0x45 | DH | RSA | Camellia-CBC(128) |
| DHE-RSA-CAMELLIA256-SHA
SHA1 | 0x00, 0x88 | DH | RSA | Camellia-CBC(256) |
| ECDHE-RSA-AES128-SHA | 0xC0, 0x13 | ECDH | RSA | AES-CBC(128) [...] |

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 recommended cipher suites.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/25/smtp

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 |
|----------------------------|------------|-------|------|-------------------|------|
| ----- | ----- | ---- | ---- | ----- | ---- |
| DHE-RSA-AES-128-CCM-AEAD | 0xC0, 0x9E | DH | RSA | AES-CCM(128) | |
| AEAD | | | | | |
| DHE-RSA-AES-128-CCM8-AEAD | 0xC0, 0xA2 | DH | RSA | AES-CCM8(128) | |
| AEAD | | | | | |
| DHE-RSA-AES128-SHA256 | 0x00, 0x9E | DH | RSA | AES-GCM(128) | |
| SHA256 | | | | | |
| DHE-RSA-AES-256-CCM-AEAD | 0xC0, 0x9F | DH | RSA | AES-CCM(256) | |
| AEAD | | | | | |
| DHE-RSA-AES-256-CCM8-AEAD | 0xC0, 0xA3 | DH | RSA | AES-CCM8(256) | |
| AEAD | | | | | |
| DHE-RSA-AES256-SHA384 | 0x00, 0x9F | DH | RSA | AES-GCM(256) | |
| SHA384 | | | | | |
| DH-AES128-SHA256 | 0x00, 0xA6 | DH | None | AES-GCM(128) | |
| SHA256 | | | | | |
| DH-AES256-SHA384 | 0x00, 0xA7 | DH | None | AES-GCM(256) | |
| SHA384 | | | | | |
| ECDHE-RSA-CAMELLIA-CBC-128 | 0xC0, 0x76 | ECDH | RSA | Camellia-CBC(128) | |
| SHA256 | | | | | |
| ECDHE-RSA-CAMELLIA-CBC-256 | 0xC0, 0x77 | ECDH | RSA | Camellia-CBC(256) | |
| SHA384 | | | | | |
| RSA-AES-128-CCM-AEAD | 0xC0, 0x9C | RSA | RSA | AES-CCM(128) | |
| AEAD | | | | | |
| RSA-AES-128-CCM8-AEAD | 0xC0, 0xA0 | RSA | RSA | AES-CCM8(128) | |
| AEAD | | | | | |
| RSA-AES128-SHA256 | 0x00, 0x9C | RSA | RSA | AES-GCM(128) | |
| SHA256 | | | | | |
| RSA-AES-256-CCM-AEAD | 0xC0, 0x9D | RSA | RSA | AES-CCM(256) | |
| AEAD | | | | | |
| RSA-AES-256-CCM8-AEAD | 0xC0, 0xA1 | RSA | RSA | AES-CCM8(256) | |
| AEAD | | | | | |
| RSA-AES256-SHA384 | 0x00, 0x9D | RSA | RSA | AES-GCM(256) | |
| SHA384 | | | | | |
| DHE-RSA-AES128-SHA | 0x00, 0x33 | [...] | | | |

25240 - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

<https://www.samba.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2022/10/12

Plugin Output

tcp/445/cifs

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/21/ftp

```
An FTP 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/25/smtp

```
An SMTP 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/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/3128/http_proxy

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

tcp/3128/http_proxy

```
An HTTP proxy is running on this port.
```


11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/22/ssh

```
An SSH server seems to be running on this port.
```

49692 - Squid Proxy Version Detection

Synopsis

It was possible to obtain the version number of the remote Squid proxy server.

Description

The remote host is running the Squid proxy server, an open source proxy server. It was possible to read the version number from the banner.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/09/28, Modified: 2024/06/17

Plugin Output

tcp/3128/http_proxy

```
URL      : http://10.0.0.112:3128/  
Version  : 5.9  
Source   : Server: squid/5.9
```

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/25/smtp

```
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/25/smtp

```
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/25/smtp

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

117885 - Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but there were intermittent authentication failures.

Description

Nessus was able to successfully authenticate to the remote host on an authentication protocol at least once using credentials provided in the scan policy.

However, one or more plugins failed to authenticate to the remote host on the same port and protocol using the same credential set that was previously successful. This may indicate an intermittent authentication problem with the remote host, which could be caused by session rate limits, session concurrency limits, or other issues preventing consistent authentication success.

These intermittent authentication failures may have affected the results of some plugins. See plugin output for failure details.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2018/10/02, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to successfully log into the remote host as :
```

```
User:      'student'  
Port:      22  
Proto:     SSH
```

```
Successful authentication was reported by the following plugin :
```

```
Plugin      : ssh_rate_limiting.nasl  
Plugin ID   : 122501
```

Plugin Name : SSH Rate Limited Device

However, one or more subsequent plugins failed to authenticate to the remote host on the same port and protocol using the same credential set that previously succeeded. This may indicate an intermittent authentication problem with the remote host which may have affected the results of the following plugins.

Error message statistics :

2 open_connection() failed on previously successful connection: Failed to open a socket on port 22.

Failure Details :

```
- Plugin      : ssh_get_info2.nasl
  Plugin ID   : 97993
  Plugin Name : OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH
  Library)
  Message     :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.

- Plugin      : bash_remote_code_execution.nasl
  Plugin ID   : 77823
  Plugin Name : Bash Remote Code Execution (Shellshock)
  Message     :
open_connection() failed on previously successful connection: Failed to open a socket on port 22.
```


141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

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

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :
```

```
User:      'student'  
Port:      22  
Proto:     SSH
```

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 10.0.0.141 to 10.0.0.112 :
10.0.0.141
10.0.0.112

Hop Count: 1
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vulnerabilities that exist on the remote host.

See Also

<https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2025/03/11

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 7 NetBIOS names have been gathered :
```

```
RIS430-TARGET    = Computer name
RIS430-TARGET    = Messenger Service
RIS430-TARGET    = File Server Service
__MSBROWSE__     = Master Browser
WORKGROUP        = Workgroup / Domain name
WORKGROUP        = Master Browser
WORKGROUP        = Browser Service Elections
```

```
This SMB server seems to be a Samba server - its MAC address is NULL.
```

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      : RIS430-Target.local.
- Advertised services :
  o Service name      : RIS430-TARGET._smb._tcp.local.
    Port number       : 445
  o Service name      : RIS430-TARGET._device-info._tcp.local.
    Port number       : 0
```

52703 - vsftpd Detection

Synopsis

An FTP server is listening on the remote port.

Description

The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.

See Also

<http://vsftpd.beasts.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/03/17, Modified: 2019/11/22

Plugin Output

tcp/21/ftp

```
Source  : 220 (vsFTPd 3.0.5)
Version : 3.0.5
```

10.0.0.116



Scan Information

Start time: Fri Mar 21 13:09:31 2025

End time: Fri Mar 21 13:12:53 2025

Host Information

IP: 10.0.0.116

MAC Address: 00:0C:29:CB:4D:D5

OS: 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

<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/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 : CN=gsm.gbuser.net/OU=Vulnerability Management Team/O=Greenbone AG Customer/L=Osnabrueck/  
ST=Niedersachsen/C=DE  
| -Issuer : CN=gsm.gbuser.net/OU=Vulnerability Management Team/O=Greenbone AG Customer/L=Osnabrueck/  
ST=Niedersachsen/C=DE
```

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/443/www

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=gsm.gbuser.net/OU=Vulnerability Management Team/O=Greenbone AG Customer/L=Osnabrueck/  
ST=Niedersachsen/C=DE
```

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

2.9

EPSS Score

0.0045

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: 2025/03/13

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:nginx:nginx -> Nginx
```

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: 2025/03/12

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 :

00:0C:29:CB:4D:D5 : VMware, Inc.

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:0C:29:CB:4D:D5
```


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
Server: nginx
Date: Fri, 21 Mar 2025 17:09:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1822
Connection: close
Last-Modified: Tue, 03 Sep 2024 14:54:35 GMT
Expires: Fri, 28 Mar 2025 17:09:59 GMT
Expires: -1
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none'; connect-src
'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'; frame-ancestors 'none'; form-
action 'self'; style-src-elem 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src
'self'; img-src 'self' blob;;
Access-Control-Allow-Origin: gsm.gbuser.net
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
```

X-Frame-Options: DENY

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :  
nginx
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :  
nginx
```

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/1.1 301 Moved Permanently

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 :

Server: nginx

Date: Fri, 21 Mar 2025 17:10:13 GMT

Content-Type: text/html

Content-Length: 162

Connection: keep-alive

Location: https://10.0.0.116/

Access-Control-Allow-Origin: gsm.gbuser.net

Access-Control-Allow-Credentials: true

Access-Control-Allow-Headers: content-type

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: DENY

Response Body :

<html>

<head><title>301 Moved Permanently</title></head>

```
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</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 : no
```

```
Options allowed : (Not implemented)
```

```
Headers :
```

```
Server: nginx
```

```
Date: Fri, 21 Mar 2025 17:10:14 GMT
```

```
Content-Type: text/html; charset=utf-8
```

```
Content-Length: 1822
```

```
Connection: keep-alive
```

```
Last-Modified: Tue, 03 Sep 2024 14:54:35 GMT
```

```
Expires: Fri, 28 Mar 2025 17:10:14 GMT
```

```
Expires: -1
```

```
Cache-Control: no-cache, no-store
```

```
Pragma: no-cache
```

```
X-Frame-Options: SAMEORIGIN
```

```
Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none'; connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'; frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self'; img-src 'self' blob;;
```

```
Access-Control-Allow-Origin: gsm.gbuser.net
```

```
Access-Control-Allow-Credentials: true
```

```
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
```

Response Body :

```
<!doctype html>
<html>
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" href="/img/favicon.png" type="image/png"/>
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Greenbone Enterprise Appliance</title>
    <script type="text/javascript" src="/config.js"></script>
    <script type="module" crossorigin src="/assets/index-8Xh5DHjy.js"></script>
    <link rel="stylesheet" crossorigin href="/assets/index-DTH69syH.css">
    <script type="module">import.meta.url;import("_").catch(()=>1);(async function*(){})(
    ).next();if(location.protocol!="file:"){window.__vite_is_modern_browser=true}</script>
    <script type="module">!function(){if(window.__vite_is_modern_browser)return;console.warn("vite:
    loading legacy chunks, syntax error above and the same error below
    should be ignored");var e=document.getElementById("vite-legacy-
    polyfill"),n=document.createElement("script");n.src=e.src,n.onload=function(){System.import(docum
    [...]
```


Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

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
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

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
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 164.842 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:09 EDT (UTC -04:00)
Scan duration : 173 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Cisco SIP Device
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W64240:00204ffff:M1460:
P2:B10113:F0x12:W65160:00204ffff0402080affffff4445414401030307:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191003_7_p=80

Following fingerprints could not be used to determine OS :
HTTP:!:Server: nginx

SSLCert:!:i/CN:gsm.gbuser.neti/O:Greenbone AG Customeri/OU:Vulnerability Management Teams/
CN:gsm.gbuser.nets/O:Greenbone AG Customers/OU:Vulnerability Management Team
d3c255c6d78958dde7dad760d290e990e4c02a08

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
```

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 TLSv1.3/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: gsm.gbuser.net
Organization Unit: Vulnerability Management Team
Organization: Greenbone AG Customer
Locality: Osnabrueck
State/Province: Niedersachsen
Country: DE

Issuer Name:

Common Name: gsm.gbuser.net
Organization Unit: Vulnerability Management Team
Organization: Greenbone AG Customer
Locality: Osnabrueck
State/Province: Niedersachsen
Country: DE

Serial Number: 0C C5 B2 63 F5 6B B2 85 19 DD 46 EB 06 98 1D 52 25 62 4B D1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 07 07:40:09 2025 GMT
Not Valid After: Feb 07 07:40:09 2027 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 3072 bits
Public Key: 00 B7 EE BF 5A 5C 55 96 DA EE 17 1A B3 38 27 D0 E4 03 00 12
```


A8 1A 34 16 2E F2 D1 F2 A8 23 EA 42 1C 31 91 72 E7 65 48 70
B3 1A 9F B1 BC 85 C0 F9 16 D4 72 44 09 FA A2 92 2A B2 5C D8
C3 51 A7 6A 0E C8 EE 21 26 19 3A DB 95 53 1B EE 01 EF 1F BD
A5 B7 0F 34 41 A9 E9 C1 93 0C F6 04 06 93 C5 2C 5A 8B 37 6D
A0 37 CB 9B 45 BD DC EE CD AD 1A 30 28 1F 8C DC AB 13 E9 72
5F 43 3C 6C B8 EC AE EE 35 1B 7E 04 A0 D6 1B DB D3 E2 BF 10
55 24 0C 3E 8A 71 87 1D CA C1 81 49 A2 E4 C8 B3 82 AA 5D FF
65 BB 3B EA 2F 35 22 5B 3D 4C 06 84 C2 D8 D6 09 70 8C 5C FD
EA 35 C7 D0 17 5A D3 86 49 1D A5 0C 33 54 1F 7C E2 8C CB C3
FE E3 D8 29 78 70 52 91 EE 91 2B D3 18 68 CF CC 2B 2E 3E 50
87 EA CD 69 68 4E D2 42 69 35 76 7B 81 31 6F 2C E4 7F AC FD
B0 32 5B 59 ED 59 D5 93 D8 A5 80 1E EB 34 FE 81 19 ED 0B 69
E6 31 51 64 8A 3F 65 85 9E E0 6A 14 BA FE 25 67 C6 3D 44 65
54 9A C1 FC E9 57 BE 8A BF D7 C6 F9 69 B3 C0 24 5C AB 37 C0
83 EB 49 3B 8D E9 24 87 EF 37 32 94 08 8B 94 0E 7A BB F0 60
BE B8 DF 9E B1 89 C4 52 91 30 AA 0D 93 85 0E EE 99 F9 4F 4F
87 6E 09 E6 CD DC 55 68 72 91 09 10 A5 FD BD AE 5D 07 1F F9
8F 64 31 64 21 91 54 89 BC 48 F2 99 45 9B 01 9 [...]

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/443/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 |
|-------------------|------------|-----|------|--------------|-----|
| RSA-AES128-SHA256 | 0x00, 0x3C | RSA | RSA | AES-CBC(128) | |
| SHA256 | | | | | |
| RSA-AES256-SHA256 | 0x00, 0x3D | RSA | RSA | AES-CBC(256) | |
| SHA256 | | | | | |

The fields above are :

{Tenable ciphertype}
{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/443/www

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

```
SSL Version : TLSv13
```

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

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

```
SSL Version : TLSv12
```

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

| Name | Code | KEX | Auth | Encryption | MAC |
|-------------------|------------|-----|------|--------------|-----|
| ----- | ----- | --- | --- | ----- | --- |
| RSA-AES256-SHA384 | 0x00, 0x9D | RSA | RSA | AES-GCM(256) | |
| SHA384 | | | | | |

| | | | | |
|-----------------------------|------------|-----|-----|--------------|
| RSA-AES128-SHA256
SHA256 | 0x00, 0x3C | RSA | RSA | AES-CBC(128) |
| RSA-AES256-SHA256
SHA256 | 0x00, 0x3D | RSA | RSA | AES-CBC(256) |

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 recommended cipher suites.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

High Strength Ciphers (\geq 112-bit key)

| Name | Code | KEX | Auth | Encryption | MAC |
|-------------------|------------|------|------|--------------|------|
| ----- | ----- | ---- | ---- | ----- | ---- |
| RSA-AES256-SHA384 | 0x00, 0x9D | RSA | RSA | AES-GCM(256) | |
| SHA384 | | | | | |
| RSA-AES128-SHA256 | 0x00, 0x3C | RSA | RSA | AES-CBC(128) | |
| SHA256 | | | | | |
| RSA-AES256-SHA256 | 0x00, 0x3D | RSA | RSA | AES-CBC(256) | |
| SHA256 | | | | | |

The fields above are :

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

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.
```

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

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/html/rfc7301>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1  
h2
```

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/12/08, Modified: 2024/09/11

Plugin Output

tcp/443/www

NPN Supported Protocols:

h2
http/1.1

62564 - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>

<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
The target advertises that the following protocols are
supported over SSL / TLS:
```

```
h2
http/1.1
```

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/443/www

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/443/www

```
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 10.0.0.141 to 10.0.0.116 :  
10.0.0.141  
10.0.0.116  
  
Hop Count: 1
```


20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

The following cookie is expired :

```
Name : GSAD_SID
Path : /
Value : 0
Domain :
Version : 1
Expires : Fri, 21 Mar 2025 17:10:07 GMT
Comment :
Secure : 1
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/443/www

The following cookie is expired :

```
Name : GSAD_SID
Path : /
Value : 0
Domain :
Version : 1
Expires : Fri, 21 Mar 2025 17:10:07 GMT
Comment :
Secure : 1
Httponly : 1
Port :
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

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

```
http://10.0.0.116/atcn0QX7oMLM.html
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/443/www

The following title tag will be used :
Greenbone Enterprise Appliance

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

<http://www.robotstxt.org/orig.html>

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
Contents of robots.txt :
```

```
User-agent: *  
Disallow: /
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL      : http://10.0.0.116/
Version  : unknown
source   : Server: nginx
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/443/www

```
URL      : https://10.0.0.116/
Version  : unknown
source   : Server: nginx
```


10.0.0.129



Scan Information

Start time: Fri Mar 21 13:09:36 2025
End time: Fri Mar 21 13:50:17 2025

Host Information

IP: 10.0.0.129
MAC Address: F0:86:20:09:66:36
OS: LG Electronics. LG TV 1.0

Vulnerabilities

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

<https://www.rc4nomore.com/>
<http://www.nessus.org/u?ac7327a0>
<http://cr.yp.to/talks/2013.03.12/slides.pdf>
<http://www.isg.rhul.ac.uk/tls/>
https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

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

Risk Factor

Medium

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)

CVSS v3.0 Temporal Score

6.9 (CVSS:3.0/E:U/RL:X/RC:C)

VPR Score

7.3

EPSS Score

0.9303

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

3.7 (CVSS2#E:U/RL:ND/RC:C)

References

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

Plugin Information

Published: 2013/04/05, Modified: 2025/02/18

Plugin Output

tcp/3001/www

```
List of RC4 cipher suites supported by the remote server :  
  
High Strength Ciphers (>= 112-bit key)
```

| Name | Code | KEX | Auth | Encryption | MAC |
|---------------------------|------------|------|------|------------|-----|
| ----- | ----- | --- | ---- | ----- | --- |
| ECDHE-RSA-RC4-SHA
SHA1 | 0xC0, 0x11 | ECDH | RSA | RC4 (128) | |
| RC4-SHA
SHA1 | 0x00, 0x05 | RSA | RSA | RC4 (128) | |

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/3001/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=New Jersey/O=LG Electronics U.S.A, Inc./CN=LG_TV_11e5c59461f4c44  
| -Issuer  : C=US/ST=New Jersey/O=LG Electronics U.S.A, Inc./CN=LG_TV_11e5c59461f4c44
```

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/3001/www

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 : C=US/ST=New Jersey/O=LG Electronics U.S.A, Inc./CN=LG_TV_11e5c59461f4c44
```

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/3001/www

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/3001/www

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

2.9

EPSS Score

0.0045

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.

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: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : embedded  
Confidence level : 90
```

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/1809/www

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 :

F0:86:20:09:66:36 : Arcadyan Corporation

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:  
- F0:86:20:09:66:36
```


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/3001/www

```
HTTP/1.1 200 OK
Date: Fri, 21 Mar 2025 17:12:57 GMT
Connection: close
Transfer-Encoding: chunked

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/1200/www

```
The remote web server type is :  
Linux/i686 UPnP/1,0 DLNADOC/1.50 LGE WebOS TV/Version 0.9
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/1809/www

```
The remote web server type is :  
WebOS/4.1.0 UPnP/1.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/1959/www

```
The remote web server type is :  
Neptune/1.1.3
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/9080/www

```
The remote web server type is :
```

```
NRDP/2020.1.7.0
```

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/1200/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 : no

Options allowed : (Not implemented)

Headers :

DLNADeviceName.lge.com: Living%20Room

Date: Fri, 21 Mar 2025 17:40:13 GMT

Content-Language: en

Server: Linux/i686 UPnP/1,0 DLNADOC/1.50 LGE WebOS TV/Version 0.9

Content-Length: 3578

Content-Type: text/xml; charset="utf-8"

Connection: close

Response Body :

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<root xmlns="urn:schemas-upnp-org:device-1-0" xmlns:dlna="urn:schemas-dlna-org:device-1-0"
  xmlns:pnp="http://schemas.microsoft.com/windows/pnp/2005/11" xmlns:df="http://
schemas.microsoft.com/windows/2008/09/devicefoundation">
```

```
  <specVersion>
```

```
    <major>1</major>
```

```
    <minor>0</minor>
```

```

</specVersion>
<device>
  <deviceType>urn:schemas-upnp-org:device:MediaRenderer:1</deviceType>
  <friendlyName>Living Room</friendlyName>
  <manufacturer>LG Electronics.</manufacturer>
  <manufacturerURL>http://www.lge.com</manufacturerURL>
  <modelDescription>LG WebOSTV DMRplus</modelDescription>
  <modelName>LG TV</modelName>
  <modelURL></modelURL>
  <modelName>1.0</modelName>
  <serialNumber></serialNumber>
  <UDN>uuid:3d59fc51-dc19-4796-a8aa-94d37fed754b</UDN>
  <pnp:X_compatibleId>MS_DigitalMediaDeviceClass_DMR_V001</pnp:X_compatibleId>
  <pnp:X_deviceCategory>MediaDevices</pnp:X_deviceCategory>
  <df:X_deviceCategory>Multimedia.DMR</df:X_deviceCategory>
  <df:X_modelId>LG Digital Media Renderer TV</df:X_modelId>
  <lge:X_LG_DLNA_DOC xmlns:lge="urn:lge-com:device-1-0">1.0</lge:X_LG_DLNA_DOC>
  <dlina:X_DLNA_DOC xmlns:dlina="urn:schemas-dlna-org:device-1-0">DMR-1.50</dlina:X_DLNA_DOC>
  <iconList>
    <icon>
      <mimetype>image/jpeg</mimetype>
      <width>48</width>
      <height>48</height>
      <depth>24</depth>
      <url>/dmrIcon_48.jpeg</url>
    </icon>
    <icon>
      <mimetype>image/jpeg</mimetype>
      <width>120</width>
      < [...]

```

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/1203/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 : no

Options allowed : (Not implemented)

Headers :

Date: Fri, 21 Mar 2025 17:40:21 GMT

Content-Language: en

Server: WebOS/4.0.0 UPnP/1.0

Content-Length: 1217

Content-Type: text/xml; charset="utf-8"

Connection: close

Response Body :

```
<?xml version="1.0" encoding="UTF-8"?>
<root xmlns="urn:schemas-upnp-org:device-1-0" xmlns:dlna="urn:schemas-dlna-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  <device>
    <deviceType>urn:lge:device:tv:1</deviceType>
```



```
<friendlyName>Living Room</friendlyName>
<manufacturer>LG Electronics</manufacturer>
<manufacturerURL></manufacturerURL>
<modelDescription></modelDescription>
<modelName>55UM6910PUC</modelName>
<modelURL></modelURL>
<serialNumber></serialNumber>
<UDN>uuid:2ad89329-b263-4ed1-ba61-1ad8c8a34ac3</UDN>
<wifiMac>F0:86:20:09:66:36</wifiMac>
<wiredMac>20:17:42:C4:E2:65</wiredMac>
<serviceList>
  <service>
    <serviceType>urn:lge:service:virtualSvc:1</serviceType>
    <serviceId>urn:lge:serviceId:virtualSvc-0000-0001</serviceId>
    <SCPDURL>/virtualService/2ad89329-b263-4ed1-ba61-1ad8c8a34ac3/scpd.xml</SCPDURL>
    <controlURL>/virtualService/2ad89329-b263-4ed1-ba61-1ad8c8a34ac3/control.xml</controlURL>
    <eventSubURL>/virtualService/2ad89329-b263-4ed1-ba61-1ad8c8a34ac3/event.xml</eventSubURL>
  </service>
</serviceList>
</device>
</root>
```

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/1959/www

```
Response Code : HTTP/1.1 412 Precondition Failed
```

```
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 :
```

```
    Date: Fri, 21 Mar 2025 17:40:21 GMT
```

```
    Content-Language: en
```

```
    Server: Neptune/1.1.3
```

```
    Content-Length: 0
```

```
    Connection: close
```

```
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/2035/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 : no

Options allowed : (Not implemented)

Headers :

Date: Fri, 21 Mar 2025 17:40:21 GMT

Content-Language: en

Server: WebOS/1.5 UPnP/1.0 webOSTV/1.0

Content-Length: 1225

Content-Type: text/xml; charset="utf-8"

Connection: close

Application-URL: http://10.0.0.129:36866/apps

Response Body :

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<root xmlns="urn:schemas-upnp-org:device-1-0" xmlns:dlna="urn:schemas-dlna-org:device-1-0">
```

```
  <specVersion>
```

```
    <major>1</major>
```

```
    <minor>0</minor>
```

```
  </specVersion>
```

```
  <device>
```

```
<deviceType>urn:dial-multiscreen-org:service:dial:1</deviceType>
<friendlyName>Living Room</friendlyName>
<manufacturer>LG Electronics</manufacturer>
<manufacturerURL>http://www.lge.com</manufacturerURL>
<modelDescription></modelDescription>
<modelName>55UM6910PUC</modelName>
<modelURL>http://www.lge.com</modelURL>
<modelNumber>WEBOS</modelNumber>
<serialNumber></serialNumber>
<UDN>uuid:3a5f7692-0ad1-4a39-b80a-20066c119253</UDN>
<serviceList>
  <service>
    <serviceType>urn:dial-multiscreen-org:service:dial:1</serviceType>
    <serviceId>urn:dial-multiscreen-org:serviceId:dial</serviceId>
    <SCPDURL>/WebOS_Dial/3a5f7692-0ad1-4a39-b80a-20066c119253/scpd.xml</SCPDURL>
    <controlURL>/WebOS_Dial/3a5f7692-0ad1-4a39-b80a-20066c119253/control.xml</controlURL>
    <eventSubURL>/WebOS_Dial/3a5f7692-0ad1-4a39-b80a-20066c119253/event.xml</eventSubURL>
  </service>
</serviceList>
</device>
</root>
```

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/9080/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 : no

Headers :

Date: Fri, 21 Mar 2025 13:40:11 EDT

Server: NRDP/2020.1.7.0

Connection: keep-alive

Cache-Control: no-cache

Content-Length: 9

Response Body :

status=ok

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1200/www

```
Port 1200/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1203/www

```
Port 1203/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1353

```
Port 1353/tcp was found to be open
```


Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1809/www

```
Port 1809/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/1959/www

```
Port 1959/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/2035/www

```
Port 2035/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3000/www

```
Port 3000/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3001/www

```
Port 3001/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/7000

```
Port 7000/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/9080/www

```
Port 9080/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/11111

```
Port 11111/tcp was found to be open
```


Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/18181

```
Port 18181/tcp was found to be open
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 273.201 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:09 EDT (UTC -04:00)
Scan duration : 2433 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : IBM Storwize
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : LG Electronics. LG TV 1.0
Confidence level : 90
Method : UPnP
Type : embedded
Fingerprint : unknown

Remote operating system : Linux
Confidence level : 59
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W29200:00204ffff:M1460:
P2:B10113:F0x12:W28960:00204ffff0402080affffff4445414401030307:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191003_7_p=3000

Following fingerprints could not be used to determine OS :
HTTP:!:Server: NRDP/2020.1.7.0

```
SSLcert:!.i/CN:LG_TV_11e5c59461f4c44i/O:LG Electronics U.S.A, Inc.s/CN:LG_TV_11e5c59461f4c44s/O:LG  
Electronics U.S.A, Inc.  
a0c6a1fef16e4530598d76a82fa3e8721728760
```

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 : LG Electronics. LG TV 1.0  
Confidence level : 90  
Method : UPnP
```

```
The remote host is running LG Electronics. LG TV 1.0
```

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/3001/www

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/3001/www

```
This port supports TLSv1.0/TLSv1.1/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/3001/www

```
Subject Name:

Country: US
State/Province: New Jersey
Organization: LG Electronics U.S.A, Inc.
Common Name: LG_TV_11e5c59461f4c44

Issuer Name:

Country: US
State/Province: New Jersey
Organization: LG Electronics U.S.A, Inc.
Common Name: LG_TV_11e5c59461f4c44

Serial Number: 00 CF FA 96 A1 DB E4 7B 3C

Version: 1

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 01 00:05:33 2019 GMT
Not Valid After: Dec 27 00:05:33 2038 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C3 5C 8A 7A ED 5D A1 73 6A 69 34 6A 6E 01 18 77 04 1B 03
            21 FE 86 98 E2 A2 F0 3B 45 31 38 E3 50 90 5F D1 66 5F 64 C3
            9C 1D 45 18 42 5C A1 C1 95 99 EA DC 72 97 1D 2A CA 38 C5 B0
            92 E6 AD 8D 51 52 73 7E 8D 67 08 8E 2D 9A E8 93 38 7F 50 A7
            DB 93 F3 69 38 DC B3 27 A3 DB 66 5B 02 3C A9 ED B3 32 2C 66
```

```
8B F0 D6 5D B5 85 A2 EC AA 98 5E 35 05 D4 79 C1 E1 A6 39 B0
DC 38 92 03 6E 34 E3 66 25 D1 A8 C7 B3 71 22 CF CC DB 75 60
7F 99 4F FA 39 8E 1C F4 4B 5E 92 DA F1 39 E6 31 67 20 19 4F
06 15 BB 46 62 9D EB AF A1 74 67 03 C9 D3 0A 13 DD 57 8F BE
16 61 28 26 5E CF 6F A9 CE 36 A0 03 4A 07 0A 73 BE 72 3A 4E
7D F2 4A E1 8E D1 9A 5B 45 34 8F 03 7C 32 47 DF 08 7A A0 9E
3B 17 C3 DA 84 67 B2 49 25 1D 11 FE C8 8F 23 7C 6C 05 AA FF
7C DF C9 49 BD 9D 52 D9 6F 5D 66 75 3D EC C8 69 33
```

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 BF 06 7B 81 A8 12 70 6F 3C C3 B8 07 40 85 75 64 CD 74 E3
B6 D1 46 66 8E BC 93 FB FD EF 99 12 18 3A BA 07 29 A2 BD 3D
1E A5 AF 21 FB 1F 71 75 70 F6 FA 6D 9D 46 77 99 24 3D 5F 1C
C7 6E 58 A3 35 69 BF 27 56 10 76 9A 7D 45 2F 17 1C 0F 72 B7
0F 94 28 F5 8F E1 16 61 65 42 56 E8 23 1F 16 70 30 8B FC F0
C0 A5 DE C9 C0 45 D3 F5 86 87 F4 7B BF C0 6C 20 BF A5 00 4D
2D 0A 2D A8 F6 FA 02 B1 15 CB 68 A1 6A A0 C3 A1 39 0F 95 04
A0 17 F3 F6 [...]

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/3001/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 SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)	
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)	
CAMELLIA128-SHA SHA1	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	

CAMELLIA256-SHA SHA1	0x00, 0x84	RSA	RSA	Camellia-CBC(256)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)

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/3001/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 SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x30	ECDH	RSA	AES-GCM(256)	
RSA-AES128-SHA256 SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	
RSA-AES256-SHA384 SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
ECDHE-RSA-AES128-SHA SHA1	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
ECDHE-RSA-AES256-SHA SHA1	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
ECDHE-RSA-RC4-SHA SHA1	0xC0, 0x11	ECDH	RSA	RC4(128)	

AES128-SHA SHA1	0x00, 0x2F	RSA	RSA	AES-CBC(128)
AES256-SHA SHA1	0x00, 0x35	RSA	RSA	AES-CBC(256)
CAMELLIA128-SHA SHA1	0x00, 0x41	RSA	RSA	Camellia-CBC(128)
CAMELLIA256-SHA SHA1	0x00, 0x84	RSA	RSA	Camellia-CBC(256)
RC4-SHA SHA1	0x00, 0x05	RSA	RSA	RC4(128)
ECDHE-RSA-AES128-SHA256 SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
ECDHE-RSA-AES256-SHA384 SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)
RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)

SSL Version : TLSv11
High [...]

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/3001/www

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

High Strength Ciphers (>= 112-bit key)

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

ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)
SHA256				
ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)
SHA384				

The fields above are :

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

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 recommended cipher suites.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/3001/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
-----	-----	----	----	-----	----
RSA-AES128-SHA256	0x00, 0x9C	RSA	RSA	AES-GCM(128)	
SHA256					
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
SHA384					
ECDHE-RSA-AES128-SHA	0xC0, 0x13	ECDH	RSA	AES-CBC(128)	
SHA1					
ECDHE-RSA-AES256-SHA	0xC0, 0x14	ECDH	RSA	AES-CBC(256)	
SHA1					
ECDHE-RSA-RC4-SHA	0xC0, 0x11	ECDH	RSA	RC4(128)	
SHA1					
AES128-SHA	0x00, 0x2F	RSA	RSA	AES-CBC(128)	
SHA1					
AES256-SHA	0x00, 0x35	RSA	RSA	AES-CBC(256)	
SHA1					
CAMELLIA128-SHA	0x00, 0x41	RSA	RSA	Camellia-CBC(128)	
SHA1					
CAMELLIA256-SHA	0x00, 0x84	RSA	RSA	Camellia-CBC(256)	
SHA1					
RC4-SHA	0x00, 0x05	RSA	RSA	RC4(128)	
SHA1					
ECDHE-RSA-AES128-SHA256	0xC0, 0x27	ECDH	RSA	AES-CBC(128)	
SHA256					
ECDHE-RSA-AES256-SHA384	0xC0, 0x28	ECDH	RSA	AES-CBC(256)	
SHA384					
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	
SHA256					
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	
SHA256					

The fields above are :

```
{Tenable ciphernam}
{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/1200/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/1203/www

```
The service closed the connection without sending any data.  
It might be protected by some sort of TCP wrapper.
```

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/1353

```
The service closed the connection without sending any data.  
It might be protected by some sort of TCP wrapper.
```

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/1809/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/1959/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/2035/www

```
The service closed the connection without sending any data.  
It might be protected by some sort of TCP wrapper.
```


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/3000/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/3001/www

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

tcp/3001/www

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

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/9080/www

```
A web server is running 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

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/12/08, Modified: 2024/09/11

Plugin Output

tcp/3001/www

NPN Supported Protocols:

```
http/1.1
http/1.0
```

62564 - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>

<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/3001/www

```
The target advertises that the following protocols are
supported over SSL / TLS:
```

```
  http/1.0
  http/1.1
```

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/3001/www

```
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/3001/www

```
TLSv1.2 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 10.0.0.141 to 10.0.0.129 :  
10.0.0.141  
10.0.0.129  
  
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://10.0.0.129:9080
http://10.0.0.129:1203/
http://10.0.0.129:1200/
http://10.0.0.129:2035/
http://10.0.0.129:1809/
```

And advertises these unique service names :

```
uuid:LGTV20193=31006035585::upnp:rootdevice
uuid:LGTV20193=31006035585::urn:schemas-upnp-org:device:mdxdevice:1
uuid:LGTV20193=31006035585::urn:mdx-netflix-com:service:target:3
uuid:2ad89329-b263-4ed1-ba61-1ad8c8a34ac3::upnp:rootdevice
uuid:2ad89329-b263-4ed1-ba61-1ad8c8a34ac3::urn:lge:device:tv:1
uuid:3d59fc51-dc19-4796-a8aa-94d37fed754b::upnp:rootdevice
uuid:2ad89329-b263-4ed1-ba61-1ad8c8a34ac3::urn:lge:service:virtualSvc:1
uuid:3d59fc51-dc19-4796-a8aa-94d37fed754b::urn:schemas-upnp-org:device:MediaRenderer:1
uuid:3d59fc51-dc19-4796-a8aa-94d37fed754b::urn:schemas-upnp-org:service:AVTransport:1
```

```
uuid:3d59fc51-dc19-4796-a8aa-94d37fed754b::urn:schemas-upnp-org:service:ConnectionManager:1
uuid:3d59fc51-dc19-4796-a8aa-94d37fed754b::urn:schemas-upnp-org:service:RenderingControl:1
uuid:3a5f7692-0ad1-4a39-b80a-20066c119253::upnp:rootdevice
uuid:c97656db-de27-15fe-052f-05f118c3788b::upnp:rootdevice
uuid:3a5f7692-0ad1-4a39-b80a-20066c119253::urn:dial-multiscreen-org:service:dial:1
uuid:c97656db-de27-15fe-052f-05f118c3788b::urn:schemas-upnp-org:device:Basic:1
uuid:c97656db-de27-15fe-052f-05f118c3788b::urn:lge-com:service:webos-second-screen:1
```

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/1200/www

```
Here is a summary of http://10.0.0.129:1200/ :

deviceType: urn:schemas-upnp-org:device:MediaRenderer:1
friendlyName: Living Room
manufacturer: LG Electronics.
manufacturerURL: http://www.lge.com
modelName: LG TV
modelDescription: LG WebOSTV DMRplus
modelName: LG TV
modelNumber: 1.0
modelURL:
serialNumber:
ServiceID: urn:upnp-org:serviceId:AVTransport
serviceType: urn:schemas-upnp-org:service:AVTransport:1
controlURL: /AVTransport/3d59fc51-dc19-4796-a8aa-94d37fed754b/control.xml
eventSubURL: /AVTransport/3d59fc51-dc19-4796-a8aa-94d37fed754b/event.xml
SCPDURL: /AVTransport/3d59fc51-dc19-4796-a8aa-94d37fed754b/scpd.xml
ServiceID: urn:upnp-org:serviceId:ConnectionManager
serviceType: urn:schemas-upnp-org:service:ConnectionManager:1
controlURL: /ConnectionManager/3d59fc51-dc19-4796-a8aa-94d37fed754b/control.xml
eventSubURL: /ConnectionManager/3d59fc51-dc19-4796-a8aa-94d37fed754b/event.xml
SCPDURL: /ConnectionManager/3d59fc51-dc19-4796-a8aa-94d37fed754b/scpd.xml
ServiceID: urn:upnp-org:serviceId:RenderingControl
```

```
serviceType: urn:schemas-upnp-org:service:RenderingControl:1
controlURL: /RenderingControl/3d59fc51-dc19-4796-a8aa-94d37fed754b/control.xml
eventSubURL: /RenderingControl/3d59fc51-dc19-4796-a8aa-94d37fed754b/event.xml
SCPDURL: /RenderingControl/3d59fc51-dc19-4796-a8aa-94d37fed754b/scpd.xml
```

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/1203/www

```
Here is a summary of http://10.0.0.129:1203/ :

deviceType: urn:lge:device:tv:1
friendlyName: Living Room
manufacturer: LG Electronics
manufacturerURL:
modelName: 55UM6910PUC
modelDescription:
modelName: 55UM6910PUC
modelURL:
serialNumber:
ServiceID: urn:lge:serviceId:virtualSvc-0000-0001
serviceType: urn:lge:service:virtualSvc:1
controlURL: /virtualService/2ad89329-b263-4ed1-ba61-1ad8c8a34ac3/control.xml
eventSubURL: /virtualService/2ad89329-b263-4ed1-ba61-1ad8c8a34ac3/event.xml
SCPDURL: /virtualService/2ad89329-b263-4ed1-ba61-1ad8c8a34ac3/scpd.xml
```

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/1809/www

```
Here is a summary of http://10.0.0.129:1809/ :

deviceType: urn:schemas-upnp-org:device:Basic:1
friendlyName: Living Room
manufacturer: LG Electronics
manufacturerURL: http://www.lge.com
modelName: LG Smart TV
modelDescription:
modelName: LG Smart TV
modelNumber: 55UM6910PUC
modelURL: http://www.lge.com
serialNumber:
ServiceID: urn:lge-com:serviceId:webos-second-screen-3000-3001
serviceType: urn:lge-com:service:webos-second-screen:1
controlURL: /WebOS_SecondScreen/c97656db-de27-15fe-052f-05f118c3788b/control.xml
eventSubURL: /WebOS_SecondScreen/c97656db-de27-15fe-052f-05f118c3788b/event.xml
SCPDURL: /WebOS_SecondScreen/c97656db-de27-15fe-052f-05f118c3788b/scpd.xml
```

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/2035/www

```
Here is a summary of http://10.0.0.129:2035/ :

deviceType: urn:dial-multiscreen-org:service:dial:1
friendlyName: Living Room
manufacturer: LG Electronics
manufacturerURL: http://www.lge.com
modelName: 55UM6910PUC
modelDescription:
modelName: 55UM6910PUC
modelNumber: WEBOS
modelURL: http://www.lge.com
serialNumber:
ServiceID: urn:dial-multiscreen-org:serviceId:dial
serviceType: urn:dial-multiscreen-org:service:dial:1
controlURL: /WebOS_Dial/3a5f7692-0ad1-4a39-b80a-20066c119253/control.xml
eventSubURL: /WebOS_Dial/3a5f7692-0ad1-4a39-b80a-20066c119253/event.xml
SCPDURL: /WebOS_Dial/3a5f7692-0ad1-4a39-b80a-20066c119253/scpd.xml
```


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      : LGwebOSTV.local.  
  
- Advertised services :  
  o Service name     : LG webOS TV FE4F._hap._tcp.local.  
    Port number      : 37142  
  o Service name     : Living Room._airplay._tcp.local.  
    Port number      : 7000
```

10.0.0.141



Scan Information

Start time: Fri Mar 21 13:09:41 2025
End time: Fri Mar 21 13:21:12 2025

Host Information

IP: 10.0.0.141
MAC Address: 00:0C:29:AA:8F:F9
OS: Linux Kernel 6.11.2-amd64

Vulnerabilities

190856 - Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities (Wednesday February 14 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.19.1, 20.11.1, 21.6.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday February 14 2024 Security Releases advisory.

- On Linux, Node.js ignores certain environment variables if those may have been set by an unprivileged user while the process is running with elevated privileges with the only exception of CAP_NET_BIND_SERVICE. Due to a bug in the implementation of this exception, Node.js incorrectly applies this exception even when certain other capabilities have been set. This allows unprivileged users to inject code that inherits the process's elevated privileges. Impacts: Thank you, to Tobias Nien for reporting this vulnerability and for fixing it. (CVE-2024-21892)
- A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to resource exhaustion and denial of service (DoS). The server reads an unbounded number of bytes from a single connection, exploiting the lack of limitations on chunk extension bytes. The issue can cause CPU and network bandwidth exhaustion, bypassing standard safeguards like timeouts and body size limits. Impacts: Thank you, to Bartek Nowotarski for reporting this vulnerability and thank you Paolo Insogna for fixing it. (CVE-2024-22019)

- The permission model protects itself against path traversal attacks by calling `path.resolve()` on any paths given by the user. If the path is to be treated as a Buffer, the implementation uses `Buffer.from()` to obtain a Buffer from the result of `path.resolve()`. By monkey-patching Buffer internals, namely, `Buffer.prototype.utf8Write`, the application can modify the result of `path.resolve()`, which leads to a path traversal vulnerability. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Niesen for reporting this vulnerability and for fixing it. (CVE-2024-21896)

- `setuid()` does not affect libuv's internal `io_uring` operations if initialized before the call to `setuid()`.

This allows the process to perform privileged operations despite presumably having dropped such privileges through a call to `setuid()`. Impacts: Thank you, to valette for reporting this vulnerability and thank you Tobias Niesen for fixing it. (CVE-2024-22017)

- A vulnerability in the `privateDecrypt()` API of the crypto library, allowed a covert timing side-channel during PKCS#1 v1.5 padding error handling. The vulnerability revealed significant timing differences in decryption for valid and invalid ciphertexts. This poses a serious threat as attackers could remotely exploit the vulnerability to decrypt captured RSA ciphertexts or forge signatures, especially in scenarios involving API endpoints processing Json Web Encryption messages. Impacts: Thank you, to hkario for reporting this vulnerability and thank you Michael Dawson for fixing it. (CVE-2023-46809)

- Node.js depends on multiple built-in utility functions to normalize paths provided to `node:fs` functions, which can be overwritten with user-defined implementations leading to filesystem permission model bypass through path traversal attack. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to xion for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21891)

- The Node.js Permission Model does not clarify in the documentation that wildcards should be only used as the last character of a file path. For example: `--allow-fs-read=/home/node/.ssh/*.pub` will ignore `pub` and give access to everything after `.ssh/`. Impacts: Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Thank you, to Tobias Niesen for reporting this vulnerability and thank you Rafael Gonzaga for fixing it. (CVE-2024-21890)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?313add11>

Solution

Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.1041

CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-46809
CVE	CVE-2024-21890
CVE	CVE-2024-21891
CVE	CVE-2024-21892
CVE	CVE-2024-21896
CVE	CVE-2024-22017
CVE	CVE-2024-22019
XREF	IAVB:2024-B-0016-S

Plugin Information

Published: 2024/02/21, Modified: 2025/02/13

Plugin Output

tcp/0

```
Path          : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version  : 20.11.1
```

192945 - Node.js 18.x < 18.20.1 / 20.x < 20.12.1 / 21.x < 21.7.2 Multiple Vulnerabilities (Wednesday, April 3, 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.1, 20.12.1, 21.7.2. It is, therefore, affected by multiple vulnerabilities as referenced in the Wednesday, April 3, 2024 Security Releases advisory.

- An attacker can make the Node.js HTTP/2 server completely unavailable by sending a small amount of HTTP/2 frames packets with a few HTTP/2 frames inside. It is possible to leave some data in nhttp2 memory after reset when headers with HTTP/2 CONTINUATION frame are sent to the server and then a TCP connection is abruptly closed by the client triggering the Http2Session destructor while header frames are still being processed (and stored in memory) causing a race condition. Impacts: Thank you, to bart for reporting this vulnerability and Anna Henningsen for fixing it. (CVE-2024-27983)

- The team has identified a vulnerability in the http server of the most recent version of Node, where malformed headers can lead to HTTP request smuggling. Specifically, if a space is placed before a content-length header, it is not interpreted correctly, enabling attackers to smuggle in a second request within the body of the first. Impacts: Thank you, to bpingel for reporting this vulnerability and Paolo Insogna for fixing it. Summary The Node.js project will release new versions of the 18.x, 20.x, 21.x releases lines on or shortly after, Wednesday, April 3, 2024 in order to address: (CVE-2024-27982)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<https://nodejs.org/en/blog/vulnerability/april-2024-security-releases/>

Solution

Upgrade to Node.js version 18.20.1 / 20.12.1 / 21.7.2 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

5.0

EPSS Score

0.3545

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-27982
CVE	CVE-2024-27983
XREF	IAVB:2024-B-0033-S

Plugin Information

Published: 2024/04/05, Modified: 2024/04/19

Plugin Output

tcp/0

```
Path          : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version  : 20.12.1
```

201969 - Node.js 18.x < 18.20.4 / 20.x < 20.15.1 / 22.x < 22.4.1 Multiple Vulnerabilities (Monday, July 8, 2024 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.4, 20.15.1, 22.4.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Monday, July 8, 2024 Security Releases advisory.

- The CVE-2024-27980 was identified as an incomplete fix for the BatBadBut vulnerability. This vulnerability arises from improper handling of batch files with all possible extensions on Windows via `child_process.spawn` / `child_process.spawnSync`. A malicious command line argument can inject arbitrary commands and achieve code execution even if the shell option is not enabled. This vulnerability affects all users of `child_process.spawn` and `child_process.spawnSync` on Windows in all active release lines.

Impact: Thank you, to tianst for reporting this vulnerability and thank you RafaelGSS for fixing it.

(CVE-2024-27980)

- A security flaw in Node.js allows a bypass of network import restrictions. By embedding non-network imports in data URLs, an attacker can execute arbitrary code, compromising system security. Verified on various platforms, the vulnerability is mitigated by forbidding data URLs in network imports. Exploiting this flaw can violate network import security, posing a risk to developers and servers. Impact: Thank you, to dittyroma for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-22020)

- A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the `--allow-fs-write` flag is used. Node.js Permission Model do not operate on file descriptors, however, operations such as `fs.fchown` or `fs.fchmod` can use a read-only file descriptor to change the owner and permissions of a file. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 22. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Impact: Thank you, to 4xpl0r3r for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-36137)

- A vulnerability has been identified in Node.js, affecting users of the experimental permission model when the `--allow-fs-read` flag is used. This flaw arises from an inadequate permission model that fails to restrict file stats through the `fs.lstat` API. As a result, malicious actors can retrieve stats from files that they do not have explicit read access to. This vulnerability affects all users using the experimental permission model in Node.js 20 and Node.js 22. Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js. Impact: Thank you, to haxatron1 for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2024-22018)

- The Permission Model assumes that any path starting with two backslashes `\\` has a four-character prefix that can be ignored, which is not always true. This subtle bug leads to vulnerable edge cases. This vulnerability affects Windows users of the Node.js Permission Model in version v22.x and v20.x Impact:

Thank you, to tniessen for reporting this vulnerability and thank you RafaelGSS for fixing it.

(CVE-2024-37372)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

Solution

Upgrade to Node.js version 18.20.4 / 20.15.1 / 22.4.1 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.1 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

EPSS Score

0.0053

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2024-22018
CVE	CVE-2024-22020
CVE	CVE-2024-27980
CVE	CVE-2024-36137
CVE	CVE-2024-37372
XREF	IAVB:2024-B-0039-S
XREF	IAVB:2024-B-0083-S

Plugin Information

Published: 2024/07/08, Modified: 2025/01/24

Plugin Output

tcp/0

```
Path          : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version  : 20.15.1
```

214404 - Node.js 18.x < 18.20.6 / 20.x < 20.18.2 / 22.x < 22.13.1 / 23.x < 23.6.1 Multiple Vulnerabilities (Tuesday, January 21, 2025 Security Releases).

Synopsis

Node.js - JavaScript run-time environment is affected by multiple vulnerabilities.

Description

The version of Node.js installed on the remote host is prior to 18.20.6, 20.18.2, 22.13.1, 23.6.1. It is, therefore, affected by multiple vulnerabilities as referenced in the Tuesday, January 21, 2025 Security Releases advisory.

- A memory leak could occur when a remote peer abruptly closes the socket without sending a GOAWAY notification. Additionally, if an invalid header was detected by nghttp2, causing the connection to be terminated by the peer, the same leak was triggered. This flaw could lead to increased memory consumption and potential denial of service under certain conditions. This vulnerability affects HTTP/2 Server users on Node.js v18.x, v20.x, v22.x and v23.x. Impact: Thank you, to newtmitch for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23085)

- With the aid of the diagnostics_channel utility, an event can be hooked into whenever a worker thread is created. This is not limited only to workers but also exposes internal workers, where an instance of them can be fetched, and its constructor can be grabbed and reinstated for malicious usage. This vulnerability affects Permission Model users (--permission) on Node.js v20, v22, and v23. Impact: Thank you, to leodog896 for reporting this vulnerability and thank you RafaelGSS for fixing it. (CVE-2025-23083)

- A vulnerability has been identified in Node.js, specifically affecting the handling of drive names in the Windows environment. Certain Node.js functions do not treat drive names as special on Windows. As a result, although Node.js assumes a relative path, it actually refers to the root directory. On Windows, a path that does not start with the file separator is treated as relative to the current directory. This vulnerability affects Windows users of path.join API. Impact: Thank you, to taise for reporting this vulnerability and thank you tniessen for fixing it. (CVE-2025-23084)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

<http://www.nessus.org/u?68bc9901>

Solution

Upgrade to Node.js version 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

6.7 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.0

EPSS Score

0.0007

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2025-23083
CVE	CVE-2025-23084
CVE	CVE-2025-23085
XREF	IAVB:2025-B-0012

Plugin Information

Published: 2025/01/21, Modified: 2025/01/24

Plugin Output

tcp/0

```
Path          : /usr/lib/python3/dist-packages/playwright/driver/node
Installed version : 20.11.0
Fixed version  : 20.18.2
```

214562 - OpenJDK 8 <= 8u432 / 11.0.0 <= 11.0.25 / 17.0.0 <= 17.0.13 / 21.0.0 <= 21.0.5 / 23.0.0 <= 23.0.1 Vulnerability (2025-01-21)

Synopsis

OpenJDK is affected by a vulnerability.

Description

The version of OpenJDK installed on the remote host is 8 prior to 8u432 / 11.0.0 prior to 11.0.25 / 17.0.0 prior to 17.0.13 / 21.0.0 prior to 21.0.5 / 23.0.0 prior to 23.0.1. It is, therefore, affected by a vulnerability as referenced in the 2025-01-21 advisory.

Please Note: Java CVEs do not always include OpenJDK versions, but are confirmed separately by Tenable using the patch versions from the referenced OpenJDK security advisory.

- Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u431-perf, 11.0.25, 17.0.13, 21.0.5, 23.0.1; Oracle GraalVM for JDK: 17.0.13, 21.0.5, 23.0.1; Oracle GraalVM Enterprise Edition: 20.3.16 and 21.3.12. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. (CVE-2025-21502)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

<https://openjdk.java.net/groups/vulnerability/advisories/2025-01-21>

Solution

Upgrade to an OpenJDK version greater than 8u432 / 11.0.25 / 17.0.13 / 21.0.5 / 23.0.1

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.2 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

3.3

EPSS Score

0.0002

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2025-21502

Plugin Information

Published: 2025/01/23, Modified: 2025/01/23

Plugin Output

tcp/0

```
Path          : /usr/lib/jvm/java-21-openjdk-amd64/  
Installed version : 21.0.5  
Fixed version   : Upgrade to a version greater than 21.0.5
```

tcp/0

```
Path          : /usr/lib/jvm/java-23-openjdk-amd64/  
Installed version : 23.0.1  
Fixed version   : Upgrade to a version greater than 23.0.1
```

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/8834/www

The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :

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

141394 - Apache HTTP Server Installed (Linux)

Synopsis

The remote host has Apache HTTP Server software installed.

Description

Apache HTTP Server is installed on the remote Linux host.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0530

Plugin Information

Published: 2020/10/12, Modified: 2025/03/11

Plugin Output

tcp/0

```
Path           : /usr/sbin/apache2
Version        : 2.4.62
Associated Package : apache2-bin: /usr/sbin/apache2
Managed by OS  : True
Running        : no
```

```
Configs found :
- /etc/apache2/apache2.conf
```

```
Loaded modules :
- libphp8.2
- mod_access_compat
- mod_alias
- mod_auth_basic
- mod_authn_core
- mod_authn_file
- mod_authz_core
- mod_authz_host
```


- mod_authz_user
- mod_autoindex
- mod_deflate
- mod_dir
- mod_env
- mod_filter
- mod_mime
- mod_mpm_prefork
- mod_negotiation
- mod_reqtimeout
- mod_setenvif
- mod_status

142640 - Apache HTTP Server Site Enumeration

Synopsis

The remote host is hosting websites using Apache HTTP Server.

Description

Domain names and IP addresses from Apache HTTP Server configuration file were retrieved from the remote host. Apache HTTP Server is a webserver environment written in C. Note: Only Linux- and Unix-based hosts are currently supported by this plugin.

See Also

<https://httpd.apache.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/11/09, Modified: 2025/02/12

Plugin Output

tcp/0

```
Sites and configs present in /usr/sbin/apache2 Apache installation:
- following sites are present in /etc/apache2/apache2.conf Apache config file:
+ - *:80
```

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: 2025/03/13

Plugin Output

tcp/0

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

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

```
Following application CPE's matched on the remote system :
```

```
cpe:/a:apache:http_server:2.4.62 -> Apache Software Foundation Apache HTTP Server
cpe:/a:exiv2:exiv2:0.28.3 -> Exiv2
cpe:/a:exiv2:libexiv2:0.28.3
cpe:/a:gnupg:libgcrypt:1.11.0 -> GnuPG Libgcrypt
cpe:/a:haxx:curl:8.11.0 -> Haxx Curl
cpe:/a:haxx:libcurl:8.11.0 -> Haxx libcurl
cpe:/a:jmcnamara:sheetparse:0.66 -> John McNamara Spreadsheet::ParseExcel
cpe:/a:nginx:nginx:1.26.0 -> Nginx
cpe:/a:nginx:nginx:1.26.0-3 -> Nginx
cpe:/a:nodejs:node.js:20.11.0 -> Node.js Node.js
cpe:/a:numpy:numpy:1.26.4 -> NumPy
cpe:/a:openssl:openssl:3.0.15 -> OpenSSL Project OpenSSL
```

```
cpe:/a:openssl:openssl:3.3.1 -> OpenSSL Project OpenSSL
cpe:/a:openssl:openssl:3.3.2 -> OpenSSL Project OpenSSL
cpe:/a:oracle:openjdk:21.0.5 -> Oracle OpenJDK -
cpe:/a:oracle:openjdk:23.0.1 -> Oracle OpenJDK -
cpe:/a:php:php:8.2.24 -> PHP PHP
cpe:/a:postgresql:postgresql:17.0 -> PostgreSQL
cpe:/a:ruby-lang:ruby:3.1.2 -> Ruby-lang Ruby
cpe:/a:sqlite:sqlite -> SQLite
cpe:/a:tenable:nessus -> Tenable Nessus
cpe:/a:tenable:nessus:10.8.3 -> Tenable Nessus
cpe:/a:tukaani:xz:5.6.3 -> Tukaani XZ
cpe:/a:vim:vim:9.1 -> Vim
cpe:/a:vmware:open_vm_tools:12.4.5 -> VMware Open VM Tools
x-cpe:/a:java:jre:21.0.5
x-cpe:/a:java:jre:23.0.1
x-cpe:/a:libndp:libndp:1.9
```

182774 - Curl Installed (Linux / Unix)

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path          : /usr/bin/curl
Version       : 8.11.0
Associated Package : curl 8.11.0-1
Managed by OS : True
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/03/11

Plugin Output

tcp/0

```
Hostname : kali  
kali (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

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

Synopsis

Detected Dockerfiles on the host.

Description

The host contains Dockerfiles, text files containing instructions to build Docker images.

See Also

<https://docs.docker.com/engine/reference/builder/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/03/29, Modified: 2025/03/05

Plugin Output

tcp/0

```
Dockerfiles found: 3
- /usr/share/metasploit-framework/tools/payloads/ysoserial/Dockerfile
- /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/net-ssh-7.3.0/Dockerfile
- /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/puma-6.4.3/tools/Dockerfile
```


25203 - Enumerate IPv4 Interfaces via SSH

Synopsis

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

Description

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

Solution

Disable any unused IPv4 interfaces.

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2024/11/20

Plugin Output

tcp/0

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

- 10.0.0.141 (on interface eth0)
- 127.0.0.1 (on interface lo)

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2024/11/20

Plugin Output

tcp/0

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

```
- ::1 (on interface lo)
```

33276 - Enumerate MAC Addresses via SSH

Synopsis

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

Description

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

Solution

Disable any unused interfaces.

Risk Factor

None

Plugin Information

Published: 2008/06/30, Modified: 2022/12/20

Plugin Output

tcp/0

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

```
- 00:0c:29:aa:8f:f9 (interface eth0)
```

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
lo:
  IPv4:
    - Address : 127.0.0.1
      Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
      Prefixlen : 128
      Scope : host
      ScopeID : 0x10
eth0:
  MAC : 00:0c:29:aa:8f:f9
  IPv4:
    - Address : 10.0.0.141
      Netmask : 255.255.255.0
      Broadcast : 10.0.0.255
```

179200 - Enumerate the Network Routing configuration via SSH

Synopsis

Nessus was able to retrieve network routing information from the remote host.

Description

Nessus was able to retrieve network routing information the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

Plugin Output

tcp/0

```
Gateway Routes:
  eth0:
    ipv4_gateways:
      10.0.0.1:
        subnets:
          - 0.0.0.0/0
Interface Routes:
  eth0:
    ipv4_subnets:
      - 10.0.0.0/24
```

168980 - Enumerate the PATH Variables

Synopsis

Enumerates the PATH variable of the current scan user.

Description

Enumerates the PATH variables of the current scan user.

Solution

Ensure that directories listed here are in line with corporate policy.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2025/03/11

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :
```

```
/usr/local/sbin  
/usr/local/bin  
/usr/sbin  
/usr/bin
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

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

See Also

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
00:0C:29:AA:8F:F9 : VMware, Inc.
```

86420 - Ethernet MAC Addresses

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:  
- 00:0C:29:AA:8F:F9
```


204827 - Exiv2 Installed (Linux / Unix)

Synopsis

Exiv2 is installed on the remote Linux / Unix host.

Description

Exiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204827' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://exiv2.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path          : /usr/bin/exiv2
Version       : 0.28.3
Associated Package : exiv2 0.28.3
Managed by OS : True
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8834/www

```
The remote web server type is :  
NessusWWW
```

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/8834/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 : no

Options allowed : (Not implemented)

Headers :

Cache-Control: must-revalidate

X-Frame-Options: DENY

Content-Type: text/html

ETag: 33b83969ea564df02878548c8e223d6f

Connection: close

X-XSS-Protection: 1; mode=block

Server: NessusWWW

Date: Fri, 21 Mar 2025 17:10:12 GMT

X-Content-Type-Options: nosniff

Content-Length: 1217

Content-Security-Policy: upgrade-insecure-requests; block-all-mixed-content; form-action 'self'; frame-ancestors 'none'; frame-src https://store.tenable.com; default-src 'self'; connect-src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data:; style-src 'self' www.tenable.com; object-src 'none'; base-uri 'self';

Strict-Transport-Security: max-age=31536000

Expect-CT: max-age=0

Response Body :

```
<!doctype html>
<html lang="en">
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <meta http-equiv="Content-Security-Policy" content="upgrade-insecure-requests; block-all-
mixed-content; form-action 'self'; frame-src https://store.tenable.com; default-src 'self'; connect-
src 'self' www.tenable.com; script-src 'self' www.tenable.com; img-src 'self' data;; style-src
'self' www.tenable.com; object-src 'none'; base-uri 'self';" />
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta charset="utf-8" />
    <title>Nessus</title>
    <link rel="stylesheet" href="nessus6.css?v=1725650918429" id="theme-link" />
    <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
    <link rel="stylesheet" href="wizard_templates.css?v=b5a92dc668a0363b1ad1778b8ea10911" />
    <!--[if lt IE 11]>
      <script>
        window.location = '/unsupported6.html';
      </script>
    <![endif]-->
    <script src="nessus6.js?v=1725650918429"></script>
    <script src="pendo-client.js"></s [...]
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/03/11

Plugin Output

tcp/0

```
+ lo
+ IPv4
- Address      : 127.0.0.1
  Assign Method : static
+ IPv6
- Address      : ::1
  Assign Method : static
+ eth0
+ IPv4
- Address      : 10.0.0.141
  Assign Method : dynamic
```

147817 - Java Detection and Identification (Linux / Unix)

Synopsis

Java is installed on the remote Linux / Unix host.

Description

One or more instances of Java are installed on the remote Linux / Unix host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- This plugin attempts to detect Oracle and non-Oracle JRE instances such as Zulu Java, Amazon Corretto, AdoptOpenJDK, IBM Java, etc
- To discover instances of JRE that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

See Also

[https://en.wikipedia.org/wiki/Java_\(software_platform\)](https://en.wikipedia.org/wiki/Java_(software_platform))

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0690

Plugin Information

Published: 2021/03/16, Modified: 2025/03/05

Plugin Output

tcp/0

Nessus detected 2 installs of Java:

```
Path          : /usr/lib/jvm/java-21-openjdk-amd64/
Version       : 21.0.5
Application    : OpenJDK Java
Binary Location : /usr/lib/jvm/java-21-openjdk-amd64/bin/java
Details        : This Java install appears to be OpenJDK due to the install directory
                  name (high confidence).
Detection Method : "find" utility
```

```
Managed by OS      : True

Path                : /usr/lib/jvm/java-23-openjdk-amd64/
Version            : 23.0.1
Application         : OpenJDK Java
Binary Location    : /usr/lib/jvm/java-23-openjdk-amd64/bin/java
Details            : This Java install appears to be OpenJDK due to the install directory
                    name (high confidence).
Detection Method   : "find" utility
Managed by OS     : True
```

189990 - Jmcnamara Spreadsheet-ParseExcel Installed (Unix)

Synopsis

Jmcnamara Spreadsheet-ParseExcel is installed on the remote Unix host.

Description

Jmcnamara Spreadsheet-ParseExcel is installed on the remote Unix host.

See Also

<https://github.com/jmcnamara/spreadsheet-parseexcel>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/02/05, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path          : /usr/share/perl5/Spreadsheet/ParseExcel.pm
Version       : 0.66
Associated Package : libspreadsheet-parseexcel-perl: /usr/share/perl5/Spreadsheet/ParseExcel.pm
Managed by OS : True
```


151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

<https://gnupg.org/download/index.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/03/05

Plugin Output

tcp/0

```
Nessus detected 4 installs of Libgcrypt:

Path      : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.5.0
Version   : 1.11.0

Path      : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
Version   : 1.11.0

Path      : /lib/x86_64-linux-gnu/libgcrypt.so.20.5.0
Version   : 1.11.0

Path      : /lib/x86_64-linux-gnu/libgcrypt.so.20
Version   : 1.11.0
```

200214 - Libndp Installed (Linux / Unix)

Synopsis

Libndp is installed on the remote Linux / Unix host.

Description

Libndp is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.200214' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://github.com/jpirko/libndp>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/06/07, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path          : libndp0 1.9-1 (via package manager)
Version       : 1.9
Managed by OS : True
```

Synopsis

Use system commands to obtain the list of mounted devices on the target machine at scan time.

Description

Report the mounted devices information on the target machine at scan time using the following commands.

```
/bin/df -h /bin/lsblk /bin/mount -l
```

This plugin only reports on the tools available on the system and omits any tool that did not return information when the command was ran.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/02/03, Modified: 2023/11/27

Plugin Output

tcp/0

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            921M   0    921M   0% /dev
tmpfs           197M  1.3M  196M   1% /run
/dev/sda1       79G   23G   52G  31% /
tmpfs           983M  4.0K  983M   1% /dev/shm
tmpfs           5.0M   0    5.0M   0% /run/lock
tmpfs           1.0M   0    1.0M   0% /run/credentials/systemd-journald.service
tmpfs           1.0M   0    1.0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs           1.0M   0    1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs           1.0M   0    1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs           1.0M   0    1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs           983M  8.0K  983M   1% /tmp
tmpfs           1.0M   0    1.0M   0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs           1.0M   0    1.0M   0% /run/credentials/getty@tty1.service
tmpfs           197M  124K  197M   1% /run/user/1000

$ lsblk
NAME MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda   8:0    0 80.1G  0 disk
##sda1 8:1    0 80.1G  0 part /

$ mount -l
```

```
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=942692k,nr_inodes=235673,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=201208k,mode=755,inode64)
/dev/sda1 on / type ext4 (rw,relatime,errors=remount-ro) [root]
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2
(rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=38,pgrp=1,timeout=0,minproto=5,maxp [...])
```

193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

```
Via date: EDT -0400
Via timedatectl: Time zone: America/New_York (EDT, -0400)
Via /etc/timezone: America/New_York
Via /etc/localtime: EST5EDT,M3.2.0,M11.1.0
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote Linux host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2024/11/26

Plugin Output

tcp/0

```
----- [ User Accounts ] -----
```

```
User       : kali
Home folder : /home/kali
Start script : /usr/bin/zsh
Groups      : kali
              dip
              scanner
              lpadmin
              netdev
              users
              dialout
              wireshark
              video
              cdrom
              adm
              audio
              sudo
              kaboxer
              bluetooth
              plugdev
              floppy
```

```
----- [ System Accounts ] -----
```

```
User       : root
Home folder : /root
Start script : /usr/bin/zsh
Groups      : root
```

```
User      : daemon
Home folder : /usr/sbin
Start script : /usr/sbin/nologin
Groups     : daemon

User      : bin
Home folder : /bin
Start script : /usr/sbin/nologin
Groups     : bin

User      : sys
Home folder : /dev
Start script : /usr/sbin/nologin
Groups     : sys

User      : sync
Home folder : /bin
Start script : /bin/sync
Groups     : nogroup

User      : games
Home folder : /usr/games
Start script : /usr/sbin/nologin
Groups     : games

User      : man
Home folder : /var/cache/man
Start script : /usr/sbin/nologin
Groups     : man

User      : lp
Home folder : /var/spool/lpd
Start script : /usr/sbin/nologin
Groups     : lp

User      : mail
Home folder : /var/mail
Start script : /usr/sbin/nologin
Groups     : mail

User      : news
Home folder : /var/spool/news
Start script : /usr/sbin/nologin
Groups     : news

User      : uucp
Home folder : /var/spool/uucp
Start script : /usr/sbin/nologin
Groups     : uucp

User      : proxy
Home folder : /bin
Start script : /usr/sbin/nologin
Groups     : proxy

User      : www-data
Home folder : /var/www
Start script : /usr/sbin/nologin
Groups     : www-data

User      : backup
Home folder : /var/backups
Start script : /usr/sbin/nologin
Groups     : backup

User      : list
Home folder : /var/list
Start script : /usr/sbin/nologin
Groups     : list
```

```
User      : irc
Home folder : [...]
```


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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes (on the localhost)
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:09 EDT (UTC -04:00)
Scan duration : 689 sec
Scan for malware : no
```

10147 - Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

Description

A Nessus daemon is listening on the remote port.

See Also

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

Solution

Ensure that the remote Nessus installation has been authorized.

Risk Factor

None

References

XREF IAVT:0001-T-0673

Plugin Information

Published: 1999/10/12, Modified: 2023/02/08

Plugin Output

tcp/8834/www

```
URL      : https://10.0.0.141:8834/  
Version  : unknown
```

64582 - Netstat Connection Information

Synopsis

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

Description

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

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/13, Modified: 2023/05/23

Plugin Output

tcp/0

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/02/19

Plugin Output

tcp/8834/www

```
Port 8834/tcp was found to be open
```

178771 - Node.js Installed (Linux / UNIX)

Synopsis

Node.js is installed on the remote Linux / UNIX host.

Description

Node.js is installed on the remote Linux / UNIX host.

See Also

<https://nodejs.org>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/07/25, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path      : /usr/lib/python3/dist-packages/playwright/driver/node
Version   : 20.11.0
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Linux Kernel 6.11.2-amd64

Confidence level : 99

Method : uname

Type : general-purpose

Fingerprint : uname:Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15)
x86_64 GNU/Linux

Following fingerprints could not be used to determine OS :

HTTP:!:Server: NessusWWW

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
Authoritys/CN:kalis/O:Nessus Users Uniteds/OU:Nessus Server
62403dbc25288908449ef9c57694447fe8916c9f

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 6.11.2-amd64
Confidence level : 99
Method : uname
```

```
The remote host is running Linux Kernel 6.11.2-amd64
```


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

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

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

```
The output of "uname -a" is :
```

```
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Linux
```

```
Local checks have been enabled for this host.
```

```
The remote Debian system is :
```

```
kali-rolling
```

```
This is a Kali Linux system
```

```
OS Security Patch Assessment is available for this host.
```

```
Runtime : 2.739172 seconds
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0516

Plugin Information

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

Plugin Output

tcp/0

```
OS Security Patch Assessment is available.
```

```
Protocol : LOCAL
```

148373 - OpenJDK Java Detection (Linux / Unix)

Synopsis

A distribution of Java is installed on the remote Linux / Unix host.

Description

One or more instances of OpenJDK Java are installed on the remote host. This may include private JREs bundled with the Java Development Kit (JDK).

Notes:

- Addition information provided in plugin Java Detection and Identification (Unix)
- Additional instances of Java may be discovered by enabling thorough tests

See Also

<https://openjdk.java.net/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/04/07, Modified: 2025/02/12

Plugin Output

tcp/0

```
Path          : /usr/lib/jvm/java-21-openjdk-amd64/
Version       : 21.0.5
Binary Location : /usr/lib/jvm/java-21-openjdk-amd64/bin/java
Managed by OS  : True
```

tcp/0

```
Path          : /usr/lib/jvm/java-23-openjdk-amd64/
Version       : 23.0.1
Binary Location : /usr/lib/jvm/java-23-openjdk-amd64/bin/java
Managed by OS  : True
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

<https://openssl.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/03/05

Plugin Output

tcp/0

Nessus detected 4 installs of OpenSSL:

```
Path          : /opt/nessus/bin/openssl
Version       : 3.0.15
Associated Package : nessus
```

```
Path          : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
Version       : 3.3.1
Associated Package : libruby3.1t64
```

```
Path          : /usr/lib/x86_64-linux-gnu/libcrypto.so.3
```

```
Version      : 3.3.2
Associated Package : libssl3t64

Path         : /usr/bin/openssl
Version      : 3.3.2
Associated Package : openssl 3.3.2-2
Managed by OS : True
```

We are unable to retrieve version info from the following list of OpenSSL files. However, these installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/usr/lib/x86_64-linux-gnu/libssl.so.3

216936 - PHP Scripting Language Installed (Unix)

Synopsis

The PHP scripting language is installed on the remote Unix host.

Description

The PHP scripting language is installed on the remote Unix host.

Note: Enabling the 'Perform thorough tests' setting will search the file system much more broadly. Thorough test is required to get results on hosts running MacOS.

See Also

<https://www.php.net>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/28, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path           : /usr/bin/php8.2
Version        : 8.2.24
Associated Package : php8.2-cli: /usr/bin/php8.2
INI file       : /etc/php/8.2/cli/php.ini
INI source     : PHP binary grep
Managed by OS : True
```

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/03/03

Plugin Output

tcp/0

Successfully retrieved and stored package data.

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/03/11

Plugin Output

tcp/0

```
. You need to take the following 2 actions :
```

```
[ Node.js 18.x < 18.20.6 / 20.x < 20.18.2 / 22.x < 22.13.1 / 23.x < 23.6.1 Multiple Vulnerabilities  
(Tuesday, January 21, 2025 Security Releases). (214404) ]
```

```
+ Action to take : Upgrade to Node.js version 18.20.6 / 20.18.2 / 22.13.1 / 23.6.1 or later.
```

```
+Impact : Taking this action will resolve 17 different vulnerabilities (CVEs).
```

```
[ OpenJDK 8 <= 8u432 / 11.0.0 <= 11.0.25 / 17.0.0 <= 17.0.13 / 21.0.0 <= 21.0.5 / 23.0.0 <= 23.0.1  
Vulnerability (2025-01-21) (214562) ]
```

```
+ Action to take : Upgrade to an OpenJDK version greater than 8u432 / 11.0.25 / 17.0.13 / 21.0.5 /  
23.0.1
```


130024 - PostgreSQL Client/Server Installed (Linux)

Synopsis

One or more PostgreSQL server or client versions are available on the remote Linux host.

Description

One or more PostgreSQL server or client versions have been detected on the remote Linux host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2019/10/18, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path      : /usr/lib/postgresql/17/bin/postgres (via package manager)
Version   : 17.0
```

tcp/0

```
Path      : /usr/lib/postgresql/17/bin/psql (via package manager)
Version   : 17.0
```

202184 - Ruby Programming Language Installed (Linux)

Synopsis

The Ruby programming language is installed on the remote Linux host.

Description

The Ruby programming language is installed on the remote Linux host.

See Also

<https://ruby.org/en/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/11, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path      : package: ruby3.1  3.1.2-8.4
Version   : 3.1.2
Managed by OS : True
```

174788 - SQLite Local Detection (Linux)

Synopsis

The remote Linux host has SQLite Database software installed.

Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

See Also

<https://www.sqlite.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/26, Modified: 2025/03/05

Plugin Output

tcp/0

```
Nessus detected 2 installs of SQLite:
```

```
Path      : /usr/bin/sqlite3
Version   : unknown
```

```
Path      : /bin/sqlite3
Version   : unknown
```

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/8834/www

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

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/8834/www

```
Subject Name:

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

Issuer Name:

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

Serial Number: 00 CE 7A

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Mar 20 14:04:57 2025 GMT
Not Valid After: Mar 19 14:04:57 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C3 CC 6E E0 E5 BA E2 42 FA D8 9B 93 76 6E C0 D5 86 A0 5D
```

```
83 D5 72 C8 80 87 C3 FC 04 00 37 C4 47 48 B3 F2 29 9B AA 7F
2F F4 FB FE CD 66 03 35 D5 1B 0E F1 B3 61 C4 7A DD 17 AA 7F
1A EE B8 2B 38 72 F3 41 07 C1 7C 71 5B 6A 3D 38 0E D6 33 8B
4E DD 2E 84 DD 34 EB 66 92 AD 9A 8B E8 21 D3 21 01 6F A6 AB
8F CC 21 87 7F 4E 43 33 B3 33 1F 16 88 94 2A 06 01 90 A4 2D
DA DB 4D D9 81 27 9F 9F DD 6B 3F 24 1C 26 0C 04 7E 1C 44 C2
81 D9 CD CB 8E 65 55 FA 5A 0C 6E 19 BC B5 B9 73 34 90 BE 08
ED 2F 8E 46 72 9F 60 04 2D 81 5A 06 5D CD FD B2 66 31 E8 66
72 1C DC FE 25 EB 77 2F 1B A0 42 32 23 44 BF D2 93 33 14 76
81 59 97 E6 4F 65 82 4D 13 83 28 98 E4 8D 80 42 5D 12 A2 DF
9F 73 47 79 F4 C2 21 96 36 65 43 CE 22 38 4E A8 7C 53 5F 97
16 15 C7 AD F3 09 7E 35 99 F7 84 C1 D1 D6 4F E8 7B
```

Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits

Signature: 00 A1 5E D3 D3 98 91 37 DE C3 CD 7A 3B B5 04 09 33 1F 22 2D
AB 4E E2 A1 CD 0D B1 A7 57 56 7E D1 7D C3 77 01 92 C2 31 46
EF E3 C7 E2 13 63 19 DC 6E 67 A1 83 CB 62 9A EA D8 CE 83 38
01 25 9F D7 19 52 77 E6 71 59 6D FA B6 DE 11 3F 0A EC BB D8
12 45 45 F6 37 AE 5D 72 F9 8D 9B 46 5B 25 59 E9 DE C7 20 DD
43 BD 96 05 62 43 AC 98 70 B3 8B CE 3D 72 71 B1 91 E6 94 B1
D7 90 9A 2D 04 2B [...]

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?e17ffcd>

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

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

```
SSL Version : TLSv13
```

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

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

```
SSL Version : TLSv12
```

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
ECDHE-RSA-AES128-SHA256	0xC0, 0x2F	ECDH	RSA	AES-GCM(128)	
SHA256					

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

The fields above are :

```
{Tenable ciphertype}
{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/8834/www

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

High Strength Ciphers (>= 112-bit key)

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

The fields above are :

{Tenable ciphertype}
{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/8834/www

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

tcp/8834/www

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

Synopsis

It was possible to enumerate installed software on the remote host via SSH.

Description

Nessus was able to list the software installed on the remote host by calling the appropriate command (e.g., 'rpm -qa' on RPM-based Linux distributions, dpkg, etc.).

Solution

Remove any software that is not in compliance with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF IAVT:0001-T-0502

Plugin Information

Published: 2006/10/15, Modified: 2025/01/13

Plugin Output

tcp/0

Here is the list of packages installed on the remote Debian Linux system :

```
ii  7zip  24.08+dfsg-1  amd64  7-Zip file archiver with a high compression ratio
ii  accountsservice  23.13.9-7  amd64  query and manipulate user account information
ii  acl  2.3.2-2+b1  amd64  access control list - utilities
ii  adduser  3.137  all  add and remove users and groups
ii  adwaita-icon-theme  47.0-2  all  default icon theme of GNOME
ii  aircrack-ng  1:1.7+git20230807.4bf83f1a-2  amd64  wireless WEP/WPA cracking utilities
ii  alsa-topology-conf  1.2.5.1-3  all  ALSA topology configuration files
ii  alsa-ucm-conf  1.2.12-1  all  ALSA Use Case Manager configuration files
ii  amass  4.2.0-0kali1  amd64  In-depth DNS Enumeration and Network Mapping
ii  amass-common  4.2.0-0kali1  all  In-depth DNS Enumeration and Network Mapping
ii  amd64-microcode  3.20240820.1  amd64  Platform firmware and microcode for AMD CPUs and SoCs
ii  apache2  2.4.62-3  amd64  Apache HTTP Server
ii  apache2-bin  2.4.62-3  amd64  Apache HTTP Server (modules and other binary files)
ii  apache2-data  2.4.62-3  all  Apache HTTP Server (common files)
ii  apache2-utils  2.4.62-3  amd64  Apache HTTP Server (utility programs for web servers)
ii  apparmor  3.1.7-1+b3  amd64  user-space parser utility for AppArmor
ii  apt  2.9.10+kali1  amd64  commandline package manager
ii  apt-file  3.3  all  search for files within Debian packages (command-line interface)
ii  apt-utils  2.9.10+kali1  amd64  package management related utility programs
ii  arj  3.10.22-28  amd64  archiver for .arj files
```

```
ii  arp-scan  1.10.0-2+b1  amd64  arp scanning and fingerprinting tool
ii  arping    2.25-1  amd64  sends IP and/or ARP pings (to the MAC address)
ii  aspell    0.60.8.1-1+b2  amd64  GNU Aspell spell-checker
ii  aspell-en  2020.12.07-0-1  all   English dictionary for GNU Aspell
ii  aspnetcore-runtime-6.0  6.0.8-1  amd64
ii  aspnetcore-targeting-pack-6.0  6.0.9-1  amd64
ii  at-spi2-common  2.54.0-1  all   Ass [...]
```

42822 - Strict Transport Security (STS) Detection

Synopsis

The remote web server implements Strict Transport Security.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

The STS header line is :

Strict-Transport-Security: max-age=31536000

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/8834/www

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


110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2024/03/25

Plugin Output

tcp/0

```
Nessus was able to execute commands locally with sufficient privileges  
for all planned checks.
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

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

Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

Plugin Output

tcp/0

```
Nessus was able to execute commands on localhost.
```

163326 - Tenable Nessus Installed (Linux)

Synopsis

Tenable Nessus is installed on the remote Linux host.

Description

Tenable Nessus is installed on the remote Linux host.

See Also

<https://www.tenable.com/products/nessus>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/07/21, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path      : /opt/nessus
Version   : 10.8.3
Build     : 20010
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The host has not yet been rebooted.
```

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma
- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://xz.tukaani.org/xz-utils/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/03/05

Plugin Output

tcp/0

Nessus detected 2 installs of XZ Utils:

Path	: /usr/lib/x86_64-linux-gnu/liblzma.so.5.6.3
Version	: 5.6.3
Associated Package	: liblzma5 5.6.3-1
Confidence	: High

```
Managed by OS      : True
Version Source     : Package

Path               : /usr/bin/xz
Version            : 5.6.3
Associated Package : xz-utils 5.6.3-1
Confidence         : High
Managed by OS     : True
Version Source     : Package
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses `/bin/ps auxww` command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.1	0.6	22672	12224	?	Ss	12:51	0:01	/sbin/init splash
root	2	0.0	0.0	0	0	?	S	12:51	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	12:51	0:00	[pool_workqueue_release]
root	4	0.0	0.0	0	0	?	I<	12:51	0:00	[kworker/R-rcu_gp]
root	5	0.0	0.0	0	0	?	I<	12:51	0:00	[kworker/R-sync_wq]
root	6	0.0	0.0	0	0	?	I<	12:51	0:00	[kworker/R-slub_flushwq]
root	7	0.0	0.0	0	0	?	I<	12:51	0:00	[kworker/R-netns]
root	9	0.0	0.0	0	0	?	I<	12:51	0:00	[kworker/0:0H-events_highpri]
root	10	0.0	0.0	0	0	?	I	12:51	0:00	[kworker/0:1-events]
root	11	0.0	0.0	0	0	?	I	12:51	0:00	[kworker/u128:0-ipv6_addrconf]
root	12	0.0	0.0	0	0	?	I<	12:51	0:00	[kworker/R-mm_percpu_wq]
root	13	0.0	0.0	0	0	?	I	12:51	0:00	[rcu_tasks_kthread]
root	14	0.0	0.0	0	0	?	I	12:51	0:00	[rcu_tasks_rude_kthread]
root	15	0.0	0.0	0	0	?	I	12:51	0:00	[rcu_tasks_trace_kthread]
root	16	0.0	0.0	0	0	?	S	12:51	0:00	[ksoftirqd/0]
root	17	0.0	0.0	0	0	?	I	12:51	0:00	[rcu_preempt]
root	18	0.0	0.0	0	0	?	S	12:51	0:00	[rcu_exp_par_gp_kthread_worker/1]
root	19	0.0	0.0	0	0	?	S	12:51	0:00	[rcu_exp_gp_kthread_worker]
root	20	0.0	0.0	0	0	?	S	12:51	0:00	[migration/0]
root	21	0.0	0.0	0	0	?	S	12:51	0:00	[idle_inject/0]
root	22	0.0	0.0	0	0	?	S	12:51	0:00	[cpuhp/0]
root	23	0.0	0.0	0	0	?	S	12:51	0:00	[cpuhp/1]
root	24	0.0	0.0	0	0	?	[...]			

152742 - Unix Software Discovery Commands Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and is able to execute all commands used to find unmanaged software.

Description

Nessus was able to determine that it is possible for plugins to find and identify versions of software on the target host. Software that is not managed by the operating system is typically found and characterized using these commands. This was measured by running commands used by unmanaged software plugins and validating their output against expected results.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

Plugin Output

tcp/0

```
Unix software discovery checks are available.
```

```
Protocol : LOCAL
```

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

<https://kb.vmware.com/s/article/340>

<http://www.nessus.org/u?c0628155>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path      : /usr/bin/vmtoolsd
Version   : 12.4.5
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

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

Solution

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

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

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

<https://www.vim.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/03/05

Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:
```

```
Path      : /usr/bin/vim.tiny
Version   : 9.1
```

```
Path      : /usr/bin/vim.basic
Version   : 9.1
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://curl.se/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/03/05

Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:
```

```
Path          : /usr/lib/x86_64-linux-gnu/libcurl.so.4.8.0
Version       : 8.11.0
Associated Package : libcurl4t64

Path          : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.8.0
Version       : 8.11.0
Associated Package : libcurl3t64-gnutls
```

204828 - libexiv2 Installed (Linux / Unix)

Synopsis

libexiv2 is installed on the remote Linux / Unix host.

Description

libexiv2 is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.
- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.204828' scanner setting in Nessus 8.15.1 or later.

Please see <https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom> for more information.

See Also

<https://exiv2.org/>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/07/29, Modified: 2025/03/05

Plugin Output

tcp/0

```
Path          : /usr/lib/x86_64-linux-gnu/libexiv2.so.0.28.3
Version       : 0.28.3
Associated Package : libexiv2-28 0.28.3
Managed by OS   : True
```

136340 - nginx Installed (Linux/UNIX)

Synopsis

NGINX is installed on the remote Linux / Unix host.

Description

NGINX, a web server with load balancing capabilities, is installed on the remote Linux / Unix host.

See Also

<https://www.nginx.com>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/05/05, Modified: 2025/03/05

Plugin Output

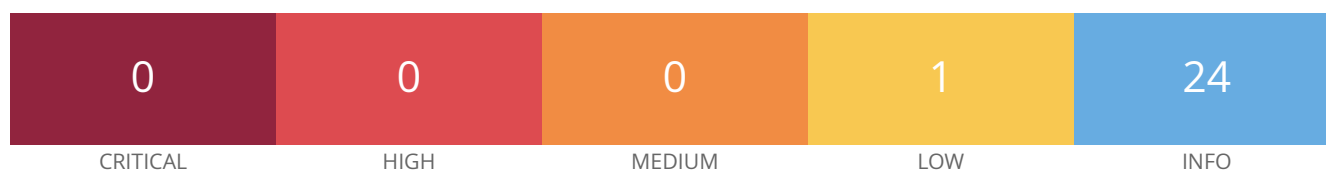
tcp/0

Nessus detected 2 installs of nginx:

```
Path      : nginx (via package manager)
Version   : 1.26.0-3

Path      : /usr/sbin/nginx
Version   : 1.26.0
Associated Package : nginx: /usr/sbin/nginx
Detection Method  : Binary in $PATH
Full Version     : 1.26.0
Managed by OS    : True
Nginx Plus       : False
```

10.0.0.175



Scan Information

Start time: Fri Mar 21 13:09:55 2025

End time: Fri Mar 21 13:14:02 2025

Host Information

IP: 10.0.0.175

MAC Address: F8:A2:D6:1C:E3:68

OS: Linux Kernel 3.1

Vulnerabilities

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

2.9

EPSS Score

0.0045

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: 2025/03/13

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: 2025/03/12

Plugin Output

tcp/0

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

19689 - Embedded Web Server Detection

Synopsis

The remote web server is embedded.

Description

The remote web server cannot host user-supplied CGIs. CGI scanning will be disabled on this server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/09/14, Modified: 2019/11/22

Plugin Output

tcp/8060/www

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 :

F8:A2:D6:1C:E3:68 : Liteon Technology Corporation

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:  
- F8:A2:D6:1C:E3:68
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/7000/www

```
The remote web server type is :  
AirTunes/377.40.00
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/8060/www

```
The remote web server type is :  
Roku/14.1.4 UPnP/1.0 Roku/14.1.4
```


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/7000/www

Response Code : HTTP/1.1 403 Forbidden

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

Server: AirTunes/377.40.00

Response Body :

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/7000/www

```
Port 7000/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8060/www

```
Port 8060/tcp was found to be open
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/43118

```
Port 43118/tcp was found to be open
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 433.536 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:10 EDT (UTC -04:00)
Scan duration : 213 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Linux Kernel 3.1
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Sharp Version: 3.4.4.61
Confidence level : 30
Method : UPnP
Type : embedded
Fingerprint : unknown

Remote operating system : Linux Kernel 2.x
Confidence level : 54
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W42340:00204ffff:M1460:
P2:B10113:F0x12:W43440:00204ffff0402080affffff4445414401030308:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191003_7_p=43118

Following fingerprints could not be used to determine OS :
HTTP:!:Server: Roku/14.1.4 UPnP/1.0 Roku/14.1.4

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 3.1  
Confidence level : 56  
Method : MLSinFP
```

```
The remote host is running Linux Kernel 3.1
```

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/7000/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/8060/www

```
The service closed the connection without sending any data.  
It might be protected by some sort of TCP wrapper.
```

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2024/11/19

Plugin Output

tcp/8060/www

```
A web server seems to be running 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

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 10.0.0.141 to 10.0.0.175 :
10.0.0.141
10.0.0.175

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://10.0.0.175:8060/  
http://10.0.0.175:8060/dial/dd.xml
```

```
And advertises these unique service names :
```

```
uuid:29780005-5c00-1011-809f-f8a2d61ce368::upnp:rootdevice  
uuid:29780005-5c00-1011-809f-f8a2d61ce368::urn:dial-multiscreen-org:service:dial:1
```

11154 - Unknown Service Detection: Banner Retrieval

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/43118

If you know what this service is and think the banner could be used to identify it, please send a description of the service along with the following output to svc-signatures@nessus.org :

```
Port      : 43118
Type      : spontaneous
Banner    :
0x00:  00 A0 00 10 70 65 72 69 70 68 65 72 61 6C 04 68    ....peripheral.h
      0x10:  6F 73 74 41 70 70 6C 69 63 61 74 69 6F 6E    ostApplication
```


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/8060/www

```
Here is a summary of http://10.0.0.175:8060/ :

deviceType: urn:roku-com:device:player:1-0
friendlyName: 55" Sharp Roku TV
manufacturer: Sharp
manufacturerURL: www.sharptvusa.com/support
modelName: 7203X
modelDescription: Roku Streaming Player Network Media
modelName: 7203X
modelNumber: 7203X
modelURL: http://www.roku.com/
serialNumber: YN005G004511
ServiceID: urn:roku-com:serviceId:ecpl-0
serviceType: urn:roku-com:service:ecp:1
controlURL:
eventSubURL:
SCPDURL: ecp_SCPD.xml
ServiceID: urn:dial-multiscreen-org:serviceId:dial1-0
serviceType: urn:dial-multiscreen-org:service:dial:1
controlURL:
eventSubURL:
SCPDURL: dial_SCPD.xml
```

tcp/8060/www

Here is a summary of `http://10.0.0.175:8060/dial/dd.xml` :

```
deviceType: urn:roku-com:device:player:1-0
friendlyName: 55" Sharp Roku TV
manufacturer: Sharp
manufacturerURL: www.sharptvusa.com/support
modelName: 7203X
modelDescription: Roku Streaming Player Network Media
modelName: 7203X
modelNumber: 7203X
modelURL: http://www.roku.com/
serialNumber: YN005G004511
ServiceID: urn:roku-com:serviceId:ecpl-0
serviceType: urn:roku-com:service:ecp:1
controlURL:
eventSubURL:
SCPDURL: ecp_SCPD.xml
ServiceID: urn:dial-multiscreen-org:serviceId:dial1-0
serviceType: urn:dial-multiscreen-org:service:dial:1
controlURL:
eventSubURL:
SCPDURL: dial_SCPD.xml
```

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

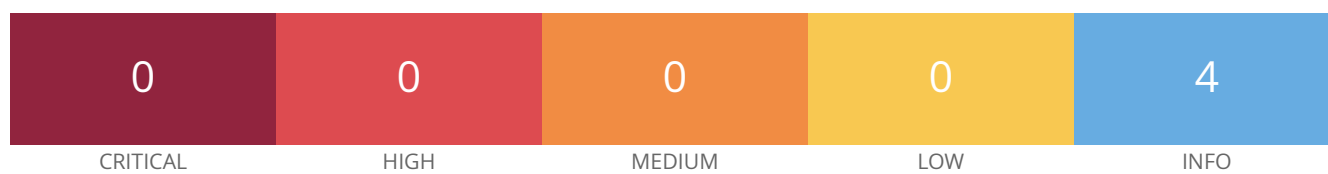
Plugin Output

udp/5353/mdns

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

```
- mDNS hostname      : YN005G004511.local.  
  
- Advertised services :  
  o Service name     : b1f110ad-55c6-5a83-a7a6-2e03773b18f2.__spotify-connect.__tcp.local.  
    Port number      : 40011  
  o Service name     : 55in Sharp Roku TV.__airplay.__tcp.local.  
    Port number      : 7000
```

10.0.0.176



Scan Information

Start time: Fri Mar 21 13:09:55 2025

End time: Fri Mar 21 13:16:40 2025

Host Information

IP: 10.0.0.176

MAC Address: 3C:A6:F6:42:8A:B1

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 :

3C:A6:F6:42:8A:B1 : Apple, 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:  
- 3C:A6:F6:42:8A:B1
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 321.746 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:10 EDT (UTC -04:00)
Scan duration : 389 sec
Scan for malware : no
```


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 10.0.0.141 to 10.0.0.176 :
10.0.0.141

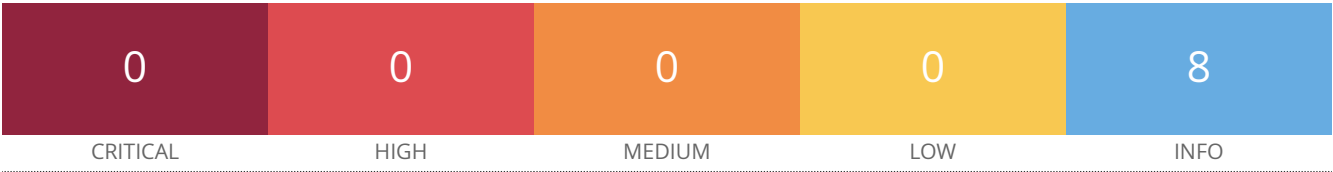
ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

10.0.0.189



Scan Information

Start time: Fri Mar 21 13:10:05 2025
End time: Fri Mar 21 13:14:22 2025

Host Information

IP: 10.0.0.189
MAC Address: EE:79:54:11:0C:BF
OS: iPhone or iPad

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: 2025/03/12

Plugin Output

tcp/0

Remote device type : embedded
Confidence level : 90

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:  
- EE:79:54:11:0C:BF
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/62078

```
Port 62078/tcp was found to be open
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 273.703 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:10 EDT (UTC -04:00)
Scan duration : 239 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : iPhone or iPad
Confidence level : 90
Method : iOS
Type : embedded
Fingerprint : unknown

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 : iPhone or iPad  
Confidence level : 90  
Method : iOS
```

```
The remote host is running iPhone or iPad
```

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

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

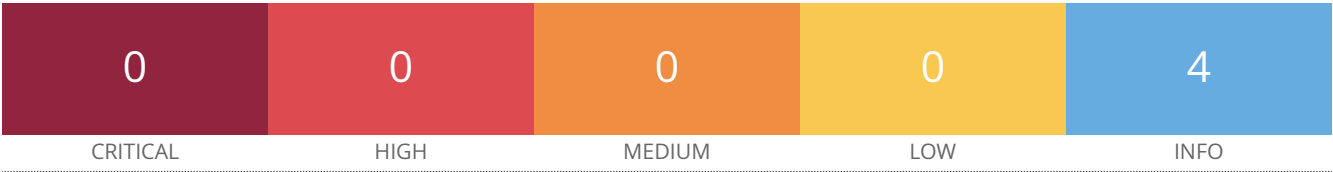
Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.0.141 to 10.0.0.189 :
10.0.0.141
10.0.0.189

Hop Count: 1
```

10.0.0.220



Scan Information

Start time: Fri Mar 21 13:10:20 2025
End time: Fri Mar 21 13:22:28 2025

Host Information

IP: 10.0.0.220
MAC Address: C0:BF:BE:4B:5D:07

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 :

C0:BF:BE:4B:5D:07 : AzureWave Technology 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:  
- C0:BF:BE:4B:5D:07
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 273.616 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:10 EDT (UTC -04:00)
Scan duration : 676 sec
Scan for malware : no
```


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 10.0.0.141 to 10.0.0.220 :
10.0.0.141

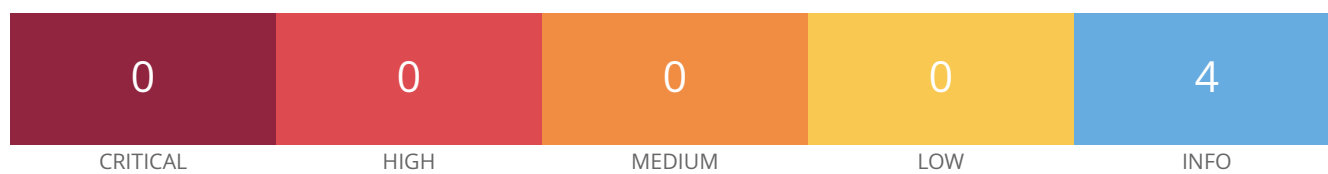
ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

10.0.0.237



Scan Information

Start time: Fri Mar 21 13:10:33 2025

End time: Fri Mar 21 13:22:28 2025

Host Information

IP: 10.0.0.237

MAC Address: A0:B3:39:5F:14:5A

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 :

A0:B3:39:5F:14:5A : Intel Corporate

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:  
- A0:B3:39:5F:14:5A
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 174.960 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:10 EDT (UTC -04:00)
Scan duration : 700 sec
Scan for malware : no
```

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 10.0.0.141 to 10.0.0.237 :
10.0.0.141

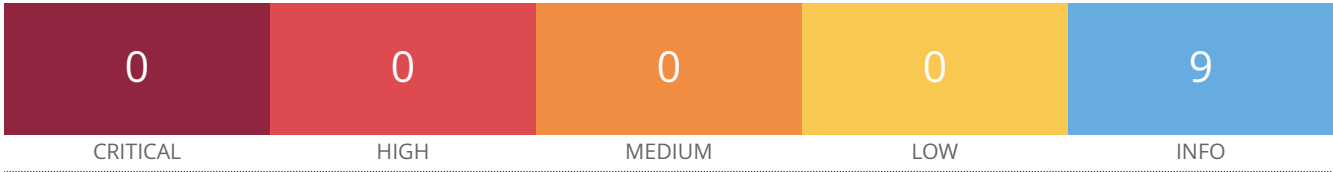
ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

10.0.0.240



Scan Information

Start time: Fri Mar 21 13:10:34 2025
End time: Fri Mar 21 13:11:43 2025

Host Information

IP: 10.0.0.240
MAC Address: DA:4E:8F:28:7C:39
OS: iPhone or iPad

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: 2025/03/12

Plugin Output

tcp/0

Remote device type : embedded
Confidence level : 90

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:  
- DA:4E:8F:28:7C:39
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/62078

```
Port 62078/tcp was found to be open
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 280.107 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:10 EDT (UTC -04:00)
Scan duration : 50 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : iPhone or iPad
Confidence level : 10
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : iPhone or iPad
Confidence level : 90
Method : iOS
Type : embedded
Fingerprint : unknown

Remote operating system : FreeBSD 6.0
FreeBSD 6.1
FreeBSD 6.2
Mac OS X 10.4
Confidence level : 54
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W65535:00204ffff:M1460:
P2:B10113:F0x12:W2896:00204ffff010303060101080affffff4445414404020000:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191003_7_p=62078

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 : iPhone or iPad  
Confidence level : 90  
Method : iOS
```

```
The remote host is running iPhone or iPad
```

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/62078

```
The service closed the connection without sending any data.  
It might be protected by some sort of TCP wrapper.
```


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

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 10.0.0.141 to 10.0.0.240 :  
10.0.0.141  
10.0.0.240  
  
Hop Count: 1
```

10.0.0.245



Scan Information

Start time: Fri Mar 21 13:10:38 2025

End time: Fri Mar 21 13:14:46 2025

Host Information

IP: 10.0.0.245

MAC Address: C0:BF:BE:4B:5D:07

OS: 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

<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/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 : CN=gsm.gbuser.net/OU=Vulnerability Management Team/O=Greenbone AG Customer/L=Osnabrueck/  
ST=Niedersachsen/C=DE  
| -Issuer : CN=gsm.gbuser.net/OU=Vulnerability Management Team/O=Greenbone AG Customer/L=Osnabrueck/  
ST=Niedersachsen/C=DE
```

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/443/www

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=gsm.gbuser.net/OU=Vulnerability Management Team/O=Greenbone AG Customer/L=Osnabrueck/  
ST=Niedersachsen/C=DE
```

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

2.9

EPSS Score

0.0045

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: 2025/03/13

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:nginx:nginx -> Nginx
```


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: 2025/03/12

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 :

C0:BF:BE:4B:5D:07 : AzureWave Technology 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:  
- C0:BF:BE:4B:5D:07
```

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
Server: nginx
Date: Fri, 21 Mar 2025 17:11:14 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1822
Connection: close
Last-Modified: Tue, 03 Sep 2024 14:54:35 GMT
Expires: Fri, 28 Mar 2025 17:11:14 GMT
Expires: -1
Cache-Control: no-cache, no-store
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none'; connect-src
'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'; frame-ancestors 'none'; form-
action 'self'; style-src-elem 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src
'self'; img-src 'self' blob;;
Access-Control-Allow-Origin: gsm.gbuser.net
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
```

X-Frame-Options: DENY

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

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :  
nginx
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :  
nginx
```

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/1.1 301 Moved Permanently

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 :

Server: nginx

Date: Fri, 21 Mar 2025 17:12:10 GMT

Content-Type: text/html

Content-Length: 162

Connection: keep-alive

Location: https://10.0.0.245/

Access-Control-Allow-Origin: gsm.gbuser.net

Access-Control-Allow-Credentials: true

Access-Control-Allow-Headers: content-type

X-Content-Type-Options: nosniff

X-XSS-Protection: 1; mode=block

X-Frame-Options: DENY

Response Body :

<html>

<head><title>301 Moved Permanently</title></head>


```
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</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 : no

Options allowed : (Not implemented)

Headers :

Server: nginx

Date: Fri, 21 Mar 2025 17:12:11 GMT

Content-Type: text/html; charset=utf-8

Content-Length: 1822

Connection: keep-alive

Last-Modified: Tue, 03 Sep 2024 14:54:35 GMT

Expires: Fri, 28 Mar 2025 17:12:10 GMT

Expires: -1

Cache-Control: no-cache, no-store

Pragma: no-cache

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: default-src 'none'; object-src 'none'; base-uri 'none'; connect-src 'self'; script-src 'self'; script-src-elem 'self' 'unsafe-inline'; frame-ancestors 'none'; form-action 'self'; style-src-elem 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self'; img-src 'self' blob;;

Access-Control-Allow-Origin: gsm.gbuser.net

Access-Control-Allow-Credentials: true

```
Access-Control-Allow-Headers: content-type
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
```

Response Body :

```
<!doctype html>
<html>
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" href="/img/favicon.png" type="image/png"/>
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Greenbone Enterprise Appliance</title>
    <script type="text/javascript" src="/config.js"></script>
    <script type="module" crossorigin src="/assets/index-8Xh5DHjy.js"></script>
    <link rel="stylesheet" crossorigin href="/assets/index-DTH69syH.css">
    <script type="module">import.meta.url;import("_").catch(()=>1);(async function*(){})(
    ).next();if(location.protocol!="file:"){window.__vite_is_modern_browser=true}</script>
    <script type="module">!function(){if(window.__vite_is_modern_browser)return;console.warn("vite:
    loading legacy chunks, syntax error above and the same error below
    should be ignored");var e=document.getElementById("vite-legacy-
    polyfill"),n=document.createElement("script");n.src=e.src,n.onload=function(){System.import(docum
    [...]
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

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
```

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

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
```

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 : 202503210446
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Software scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.0.141
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 250.801 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
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 : disabled
Web application tests : disabled
Max hosts : 192
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 : 2025/3/21 13:10 EDT (UTC -04:00)
Scan duration : 225 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

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. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

Following OS Fingerprints were found

Remote operating system : Cisco SIP Device
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W64240:00204ffff:M1460:
P2:B10113:F0x12:W65160:00204ffff0402080affffff4445414401030307:M1460:
P3:B00000:F0x00:W0:00:M0
P4:191003_7_p=80

Following fingerprints could not be used to determine OS :
HTTP:!:Server: nginx

SSLCert:!:i/CN:gsm.gbuser.neti/O:Greenbone AG Customeri/OU:Vulnerability Management Teams/
CN:gsm.gbuser.nets/O:Greenbone AG Customers/OU:Vulnerability Management Team
d3c255c6d78958dde7dad760d290e990e4c02a08

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
```

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 TLSv1.3/TLSv1.2.
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/443/www

```
Subject Name:

Common Name: gsm.gbuser.net
Organization Unit: Vulnerability Management Team
Organization: Greenbone AG Customer
Locality: Osnabrueck
State/Province: Niedersachsen
Country: DE

Issuer Name:

Common Name: gsm.gbuser.net
Organization Unit: Vulnerability Management Team
Organization: Greenbone AG Customer
Locality: Osnabrueck
State/Province: Niedersachsen
Country: DE

Serial Number: 0C C5 B2 63 F5 6B B2 85 19 DD 46 EB 06 98 1D 52 25 62 4B D1

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Feb 07 07:40:09 2025 GMT
Not Valid After: Feb 07 07:40:09 2027 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 3072 bits
Public Key: 00 B7 EE BF 5A 5C 55 96 DA EE 17 1A B3 38 27 D0 E4 03 00 12
```

A8 1A 34 16 2E F2 D1 F2 A8 23 EA 42 1C 31 91 72 E7 65 48 70
B3 1A 9F B1 BC 85 C0 F9 16 D4 72 44 09 FA A2 92 2A B2 5C D8
C3 51 A7 6A 0E C8 EE 21 26 19 3A DB 95 53 1B EE 01 EF 1F BD
A5 B7 0F 34 41 A9 E9 C1 93 0C F6 04 06 93 C5 2C 5A 8B 37 6D
A0 37 CB 9B 45 BD DC EE CD AD 1A 30 28 1F 8C DC AB 13 E9 72
5F 43 3C 6C B8 EC AE EE 35 1B 7E 04 A0 D6 1B DB D3 E2 BF 10
55 24 0C 3E 8A 71 87 1D CA C1 81 49 A2 E4 C8 B3 82 AA 5D FF
65 BB 3B EA 2F 35 22 5B 3D 4C 06 84 C2 D8 D6 09 70 8C 5C FD
EA 35 C7 D0 17 5A D3 86 49 1D A5 0C 33 54 1F 7C E2 8C CB C3
FE E3 D8 29 78 70 52 91 EE 91 2B D3 18 68 CF CC 2B 2E 3E 50
87 EA CD 69 68 4E D2 42 69 35 76 7B 81 31 6F 2C E4 7F AC FD
B0 32 5B 59 ED 59 D5 93 D8 A5 80 1E EB 34 FE 81 19 ED 0B 69
E6 31 51 64 8A 3F 65 85 9E E0 6A 14 BA FE 25 67 C6 3D 44 65
54 9A C1 FC E9 57 BE 8A BF D7 C6 F9 69 B3 C0 24 5C AB 37 C0
83 EB 49 3B 8D E9 24 87 EF 37 32 94 08 8B 94 0E 7A BB F0 60
BE B8 DF 9E B1 89 C4 52 91 30 AA 0D 93 85 0E EE 99 F9 4F 4F
87 6E 09 E6 CD DC 55 68 72 91 09 10 A5 FD BD AE 5D 07 1F F9
8F 64 31 64 21 91 54 89 BC 48 F2 99 45 9B 01 9 [...]

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/443/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
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	

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/443/www

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

```
SSL Version : TLSv13
```

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

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

```
SSL Version : TLSv12
```

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

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	---	---	-----	---
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
SHA384					

RSA-AES128-SHA256 SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)
RSA-AES256-SHA256 SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)

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 recommended cipher suites.

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/443/www

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

High Strength Ciphers (\geq 112-bit key)

Name	Code	KEX	Auth	Encryption	MAC
-----	-----	----	----	-----	----
RSA-AES256-SHA384	0x00, 0x9D	RSA	RSA	AES-GCM(256)	
SHA384					
RSA-AES128-SHA256	0x00, 0x3C	RSA	RSA	AES-CBC(128)	
SHA256					
RSA-AES256-SHA256	0x00, 0x3D	RSA	RSA	AES-CBC(256)	
SHA256					

The fields above are :

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

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.
```

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

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/html/rfc7301>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2024/09/11

Plugin Output

tcp/443/www

```
http/1.1  
h2
```

87242 - TLS NPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS NPN extension.

Description

The remote host supports the TLS NPN (Transport Layer Security Next Protocol Negotiation) extension. This plugin enumerates the protocols the extension supports.

See Also

<https://tools.ietf.org/id/draft-agl-tls-nextprotoneg-03.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/12/08, Modified: 2024/09/11

Plugin Output

tcp/443/www

NPN Supported Protocols:

h2
http/1.1

62564 - TLS Next Protocols Supported

Synopsis

The remote service advertises one or more protocols as being supported over TLS.

Description

This script detects which protocols are advertised by the remote service to be encapsulated by TLS connections.

Note that Nessus did not attempt to negotiate TLS sessions with the protocols shown. The remote service may be falsely advertising these protocols and / or failing to advertise other supported protocols.

See Also

<https://tools.ietf.org/html/draft-agl-tls-nextprotoneg-04>

<https://technotes.googlecode.com/git/nextprotoneg.html>

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2012/10/16, Modified: 2022/04/11

Plugin Output

tcp/443/www

```
The target advertises that the following protocols are
supported over SSL / TLS:
```

```
h2
http/1.1
```


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/443/www

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

Plugin Output

tcp/443/www

```
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 10.0.0.141 to 10.0.0.245 :  
10.0.0.141  
10.0.0.245  
  
Hop Count: 1
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/80/www

The following cookie is expired :

```
Name : GSAD_SID
Path : /
Value : 0
Domain :
Version : 1
Expires : Fri, 21 Mar 2025 17:11:48 GMT
Comment :
Secure : 1
Httponly : 1
Port :
```

100669 - Web Application Cookies Are Expired

Synopsis

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

Description

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

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If needed, set an expiration date in the future so the cookie will persist or remove the Expires cookie attribute altogether to convert the cookie to a session cookie.

Risk Factor

None

Plugin Information

Published: 2017/06/07, Modified: 2021/12/20

Plugin Output

tcp/443/www

The following cookie is expired :

```
Name : GSAD_SID
Path : /
Value : 0
Domain :
Version : 1
Expires : Fri, 21 Mar 2025 17:11:48 GMT
Comment :
Secure : 1
Httponly : 1
Port :
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/80/www

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

```
http://10.0.0.245/v5enyG1jtIUd.html
```

10386 - Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/443/www

The following title tag will be used :
Greenbone Enterprise Appliance

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a website for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

<http://www.robotstxt.org/orig.html>

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/443/www

```
Contents of robots.txt :
```

```
User-agent: *  
Disallow: /
```


106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL      : http://10.0.0.245/  
Version  : unknown  
source   : Server: nginx
```

106375 - nginx HTTP Server Detection

Synopsis

The nginx HTTP server was detected on the remote host.

Description

Nessus was able to detect the nginx HTTP server by looking at the HTTP banner on the remote host.

See Also

<https://nginx.org/>

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0677

Plugin Information

Published: 2018/01/26, Modified: 2023/05/24

Plugin Output

tcp/443/www

```
URL      : https://10.0.0.245/  
Version  : unknown  
source   : Server: nginx
```