tenable® Nessus

My Basic Network Scan

Vulnerabilities by Host

Vulnerabilities by Host

192.168.43.230

0	0	5	1	61
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Jan 29 03:51:44 2024
End time:	Mon Jan 29 04:02:03 2024

Host Information

IP:	192.168.43.230
MAC Address:	00:45:E2:55:38:6B
OS:	Linux Kernel 6.5.0-kali3-amd64

Vulnerabilities

187725 - Curl 7.46.0 <= 8.4.0 Information Disclosure (CVE-2023-46218)

Synopsis

The remote Windows host has a program that is affected by an information disclosure vulnerability.

Description

The version of Curl installed on the remote host is between 7.46.0 and 8.4.0. It is, therefore, affected by an information disclosure vulnerability. A mixed case flaw in Curl's function that verifies a given cookie domain against the Public Suffix List (PSL) allows a malicious HTTP server to set 'super cookies' in Curl, that are then passed back to more origins than what is otherwise allowed or possible. For example a cookie could be set with `domain=co.UK` when the URL used a lower case hostname `curl.co.uk`, even though `co.uk` is listed as a PSL domain.

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://curl.se/docs/CVE-2023-46218.html

Solution

Upgrade Curl to version 8.5.0 or later

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 v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

References

CVE   CVE-2023-46218

Plugin Information

Published: 2024/01/09, Modified: 2024/01/10

Plugin Output

tcp/0

```
Path              : /opt/lampp/bin/curl
Installed version : 7.53.1
Fixed version     : 8.5.0
```

184811 - OpenSSL 1.1.1 < 1.1.1x Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

The version of OpenSSL installed on the remote host is prior to 1.1.1x. It is, therefore, affected by a vulnerability as referenced in the 1.1.1x advisory.

- Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the -pubcheck option, as well as the OpenSSL genpkey command line application.

The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-5678)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.nessus.org/u?ed8c16ba

https://www.cve.org/CVERecord?id=CVE-2023-5678

https://www.openssl.org/news/secadv/20231106.txt

https://www.openssl.org/policies/secpolicy.html

Solution

Upgrade to OpenSSL version 1.1.1x or later.

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:N/A:L)

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:N/A:P)

CVSS v2.0 Temporal Score

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

References

CVE   CVE-2023-5678

Plugin Information

Published: 2023/11/07, Modified: 2023/11/22

Plugin Output

tcp/0

```
    Path            : /opt/lampp/bin/openssl
    Reported version : 1.1.1w
    Fixed version    : 1.1.1x
```

tcp/0

```
    Path            : /opt/lampp/lib/libcrypto.so.1.1
    Reported version : 1.1.1w
    Fixed version    : 1.1.1x
```

tcp/0

```
    Path            : /opt/lampp/lib/libssl.so.1.1
    Reported version : 1.1.1w
    Fixed version    : 1.1.1x
```

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
```

182873 - libcurl 7.9.1 < 8.4.0 Cookie Injection

Synopsis

The remote libcurl install is affected by a cookie injection vulnerability.

Description

The version of libcurl installed on the remote host is affected by a cookie injection vulnerability. This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met.

libcurl performs transfers. In its API, an application creates 'easy handles' that are the individual handles for single transfers.

libcurl provides a function call that duplicates an easy handle called curl_easy_duphandle.

If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but without cloning the actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the handle would instead store the file name as none (using the four ASCII letters, no quotes).

Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named none - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course.

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://curl.se/docs/CVE-2023-38546.html

Solution

Upgrade libcurl to version 8.4.0 or later

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

3.4 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

2.0 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

CVE   CVE-2023-38546
XREF   CEA-ID:CEA-2023-0052
XREF   IAVA:2023-A-0531-S

Plugin Information

Published: 2023/10/11, Modified: 2023/12/08

Plugin Output

tcp/0

```
Path              : /opt/lampp/lib/libcurl.so.4.4.0
Installed version : 7.53.1
Fixed version     : 8.4.0
```

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: 2024/01/16

Plugin Output

tcp/0

```
 Nessus detected 2 installs of Apache:

   Path    : /opt/lampp/bin/httpd
   Version : 2.4.58
   Running : no

   Configs found :

   Loaded modules :

   Path               : /usr/sbin/apache2
   Version            : 2.4.58
   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: 2023/12/27

Plugin Output

tcp/0

```
No sites are configured for /opt/lampp/bin/httpd Apache installation.

Sites and configs present in /usr/sbin/apache2 Apache installation:
  - following sites are present in /etc/apache2/apache2.conf Apache config file:
    +  - *:80
```

156000 - Apache Log4j Installed (Linux / Unix)

Synopsis

Apache Log4j, a logging API, is installed on the remote Linux / Unix host.

Description

One or more instances of Apache Log4j, a logging API, are installed on the remote Linux / Unix Host.

The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' 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://logging.apache.org/log4j/2.x/

Solution

n/a

Risk Factor

None

References

XREF	IAVA:0001-A-0650
XREF	IAVT:0001-T-0941

Plugin Information

Published: 2021/12/10, Modified: 2024/01/16

Plugin Output

tcp/0

```
    Path                         : /usr/share/neo4j/lib/neo4j-logging-4.4.26.jar
    Version                      : 2.17.1
    JMSAppender.class association  : Found
    JdbcAppender.class association : Found
    JndiLookup.class association   : Found
    Method                       : pom.properties dependency
```

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: 2023/12/27

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:2.4.58 -> Apache Software Foundation Apache HTTP Server
   cpe:/a:apache:log4j:2.17.1 -> Apache Software Foundation log4j
   cpe:/a:gnupg:libgcrypt:1.10.3 -> GnuPG Libgcrypt
   cpe:/a:haxx:curl:7.53.1 -> Haxx Curl
   cpe:/a:haxx:curl:8.5.0 -> Haxx Curl
   cpe:/a:haxx:libcurl:7.53.1 -> Haxx libcurl
   cpe:/a:haxx:libcurl:8.5.0 -> Haxx libcurl
   cpe:/a:nginx:nginx:1.24.0 -> Nginx
   cpe:/a:nodejs:node.js:18.19.0 -> Nodejs Node.js
   cpe:/a:openssl:openssl:1.1.1w -> OpenSSL Project OpenSSL
   cpe:/a:openssl:openssl:3.0.12 -> OpenSSL Project OpenSSL
   cpe:/a:openssl:openssl:3.1.4 -> OpenSSL Project OpenSSL
```

```
cpe:/a:oracle:openjdk:unknown -> Oracle OpenJDK -
cpe:/a:postgresql:postgresql:16.1 -> PostgreSQL
cpe:/a:sqlite:sqlite -> SQLite
cpe:/a:tenable:nessus -> Tenable Nessus
cpe:/a:tenable:nessus:10.6.4 -> Tenable Nessus
x-cpe:/a:java:jre:unknown
```

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.

Note that more paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2024/01/16

Plugin Output

tcp/0

```
Nessus detected 2 installs of Curl:

  Path              : /usr/bin/curl
  Version           : 8.5.0
  Associated Package : curl 8.5.0-2
  Managed by OS     : True

  Path    : /opt/lampp/bin/curl
  Version : 7.53.1
```

106203 - DHCP server Detection (Linux)

Synopsis

A DHCP server is installed on the remote host.

Description

A DHCP server is installed on the remote host.

See Also

https://www.isc.org/downloads/dhcp/

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0938

Plugin Information

Published: 2018/01/19, Modified: 2024/01/16

Plugin Output

tcp/0

```
    Type    : isc-dhcpd
    Version : 4.4.3.1
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2024/01/16

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: 2022/09/09

Plugin Output

tcp/0

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

159273 - Dockerfile Detection for Linux/UNIX

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: 2024/01/16

Plugin Output

tcp/0

```
Dockerfiles found: 5
 - /home/lexlikeluthor/.vscode/extensions/esbenp.prettier-vscode-10.1.0/.devcontainer/Dockerfile
 - /home/lexlikeluthor/.vscode/extensions/ms-python.python-2023.22.1/.devcontainer/Dockerfile
 - /usr/share/metasploit-framework/tools/payloads/ysoserial/Dockerfile
 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/net-ssh-7.2.1/Dockerfile
 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/puma-6.4.2/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: 2023/10/04

Plugin Output

tcp/0

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

 - 127.0.0.1 (on interface lo)
 - 192.168.43.230 (on interface wlan0)
```

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: 2022/02/23

Plugin Output

tcp/0

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

 - ::1 (on interface lo)
 - fe80::245:e2ff:fe55:386b (on interface wlan0)
```

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 :

  - 00:45:e2:55:38:6b (interface wlan0)
```

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: 2023/11/17

Plugin Output

tcp/0

```
wlan0:
  MAC : 00:45:e2:55:38:6b
  IPv4:
    - Address : 192.168.43.230
        Netmask : 255.255.255.0
        Broadcast : 192.168.43.255
  IPv6:
    - Address : fe80::245:e2ff:fe55:386b
        Prefixlen : 64
        Scope : link
        ScopeID : 0x20
lo:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
        Scope : host
        ScopeID : 0x10
```

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:
  wlan0:
    ipv4_gateways:
      192.168.43.1:
        subnets:
          - 0.0.0.0/0
Interface Routes:
  wlan0:
    ipv4_subnets:
      - 192.168.43.0/24
    ipv6_subnets:
      - fe80::/64
```

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: 2024/01/16

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 :

00:45:E2:55:38:6B : CyberTAN 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:
  - 00:45:E2:55:38:6B
```

168982 - Filepaths contain Dangerous characters (Linux)

Synopsis

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential.

Description

This Tenable product detected files or paths on the scanned Unix-like system which contain characters with command injection or privilege escalation potential. Although almost any character is valid for an entry in this kind of filesystem, such as semicolons, use of some of them may lead to problems or security compromise when used in further commands.

This product has chosen in certain plugins to avoid digging within those files and directories for security reasons.

These should be renamed to avoid security compromise.

Solution

Rename these files or folders to not include dangerous characters.

Risk Factor

None

Plugin Information

Published: 2022/12/21, Modified: 2022/12/21

Plugin Output

tcp/22

```
The following files and directories contain potentially dangerous characters such as brackets,
 ampersand, or semicolon.
This scanner avoided access to these files when possible for safety:

/usr/share/node_modules/@types/node
/usr/share/nodejs/@types/node
```

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 and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

```
Response Code : HTTP/1.1 200 OK

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

  Cache-Control: must-revalidate
  X-Frame-Options: DENY
  Content-Type: text/html
  ETag: 21c60de45a1b3054c576fc111326c7b3
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Mon, 29 Jan 2024 01:51:53 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 :
```

```html
<!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=1701889299529" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
        <link rel="stylesheet" href="wizard_templates.css?v=11939be86ca24a4dbbe8f9b85f95e140" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1701889299529"></script>
        <script src="pendo-client.js"></script>
        <!--Resource-Script-->
    </head>
    [...]
```

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: 2024/01/16

Plugin Output

tcp/0

```
 + lo
   + IPv4
     - Address       : 127.0.0.1
       Assign Method : static
   + IPv6
     - Address       : ::1
       Assign Method : static
 + wlan0
   + IPv4
     - Address       : 192.168.43.230
       Assign Method : dynamic
   + IPv6
     - Address       : fe80::245:e2ff:fe55:386b
       Assign Method : static
```

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)

Solution

n/a

Risk Factor

None

References

XREF   IAVT:0001-T-0690

Plugin Information

Published: 2021/03/16, Modified: 2024/01/22

Plugin Output

tcp/0

```
Nessus detected 2 installs of Java:

  Path              : /usr/lib/jvm/java-11-openjdk-amd64/
  Version           : Unknown
  Application       : OpenJDK Java
  Binary Location   : /usr/lib/jvm/java-11-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-17-openjdk-amd64/
Version           : Unknown
Application       : OpenJDK Java
Binary Location   : /usr/lib/jvm/java-17-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
```

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: 2024/01/16

Plugin Output

tcp/0

```
Nessus detected 4 installs of Libgcrypt:

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.4.3
  Version : 1.10.3

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.10.3

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.4.3
  Version : 1.10.3

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.10.3
```

157358 - Linux Mounted Devices

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            1.8G     0  1.8G   0% /dev
tmpfs           371M  1.5M  370M   1% /run
/dev/sda2       915G   32G  836G   4% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
efivarfs        184K  112K   68K  63% /sys/firmware/efi/efivars
/dev/sda1       511M  148K  511M   1% /boot/efi
tmpfs           371M  2.5M  369M   1% /run/user/1000


$ lsblk
NAME   MAJ:MIN RM    SIZE RO TYPE MOUNTPOINTS
sda      8:0    0 931.5G  0 disk
##sda1   8:1    0   512M  0 part /boot/efi
##sda2   8:2    0 930.1G  0 part /
##sda3   8:3    0   977M  0 part [SWAP]


$ 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=1857256k,nr_inodes=464314,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=379784k,mode=755,inode64)
/dev/sda2 on / type ext4 (rw,relatime,errors=remount-ro)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,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)
efivarfs on /sys/firmware/efi/efivars type efivarfs (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=32,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=16037)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/h [...]
```

95928 - Linux User List Enumeration

Synopsis

Nessus was able to enumerate local users and groups on the remote host.

Description

Using the supplied credentials, Nessus was able to enumerate the local users and groups on the remote host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2023/11/27

Plugin Output

tcp/0

```
----------[ User Accounts ]----------

User         : lexlikeluthor
Home folder  : /home/lexlikeluthor
Start script : /usr/bin/zsh
Groups       : dip
               scanner
               netdev
               users
               dialout
               lexlikeluthor
               wireshark
               video
               cdrom
               adm
               audio
               sudo
               kaboxer
               bluetooth
               plugdev
               floppy

User         : beef-xss
Home folder  : /var/lib/beef-xss
Start script : /usr/sbin/nologin
Groups       : beef-xss

----------[ 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       : l [...]
```

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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.4
Nessus build : 20005
Plugin feed version : 202401281258
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian10-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
```

```
Scan policy used : Basic Network Scan
Scanner IP : 192.168.43.230
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes (on the localhost)
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/1/29 3:51 CAT
Scan duration : 618 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://192.168.43.230:8834/
    Version : unknown
```

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: 2023/11/24

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: 2024/01/16

Plugin Output

tcp/0

```
Path            : /usr/bin/node
Version         : 18.19.0
Managed         : 1
Package         : nodejs
Package release : 6
Package version : 18.19.0+dfsg

aliases :
  - /bin/node
  - /bin/nodejs
  - /usr/bin/nodejs
```

178772 - Node.js Modules Installed (Linux)

Synopsis

Nessus was able to enumerate one or more Node.js modules installed on the remote host.

Description

Nessus was able to enumerate one or more Node.js modules installed on the remote host.

See Also

https://nodejs.org/api/modules.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/07/25, Modified: 2024/01/16

Plugin Output

tcp/0

```
    Installed top-level Node.js modules :

 name: acorn-dynamic-import
 version: 4.0.0
 path: /usr/share/node_modules/acorn-dynamic-import/package.json

 name: @fastify/busboy
 version: 2.1.0
 path: /usr/share/node_modules/@fastify/busboy/package.json

 name: acorn-numeric-separator
 version: 0.3.4
 path: /usr/share/node_modules/acorn-numeric-separator/package.json

 name: undici-types
 version: 5.28.2
 path: /usr/share/node_modules/undici-types/package.json

 name: @types/node
 version: 18.18.14
 path: /usr/share/node_modules/@types/node/package.json

 name: @types/busboy
 version: 1.5.0
```

```
path: /usr/share/node_modules/@types/busboy/package.json

name: acorn-class-fields
version: 1.0.0
path: /usr/share/node_modules/acorn-class-fields/package.json

name: acorn-loose
version: 8.3.0
path: /usr/share/node_modules/acorn-loose/package.json

name: acorn-import-assertions
version: 1.8.0
path: /usr/share/node_modules/acorn-import-assertions/package.json

name: normalize.css
version: 8.0.1
path: /usr/share/node_modules/normalize.css/package.json

name: busboy
version: 1.6.0
path: /usr/share/node_modules/busboy/package.json

name: acorn-private-methods
version: 1.0.0
path: /usr/share/node_modules/acorn-private-methods/package.json

name: acorn-static-class-features
version: 1.0.0
path: /usr/share/node_modules/acorn-static-class-features/package.json

name: acorn
version: 8.8.1
path: /usr/share/node_modules/acorn/package.json

name: acorn-export-ns-from
version: 0.2.0
path: /usr/share/node_modules/acorn-export-ns-from/package.json

name: undici/types
version: 5.28.2
path: /usr/share/node_modules/undici/types/package.json

name: undici
version: 5.28.2
path: /usr/share/node_modules/undici/package.json

name: xtend
version: 4.0.2
path: /usr/share/node_modules/xtend/package.json

name: acorn-walk
version: 8.2.0
path: /usr/share/node_modules/acorn-walk/package.json

name: binary-search
version: 1.3.6
path: /usr/share/node_modules/binary-search/package.json

name: acorn-jsx
version: 5.3.1
path: /usr/share/node_modules/acorn-jsx/package.json

name: [...]
```

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: 2023/11/08

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 6.5.0-kali3-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 6.5.0-kali3-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: 2023/11/28

Plugin Output

tcp/0

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

The output of "uname -a" is :
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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 : 2.37008 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
```

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: 2023/12/27

Plugin Output

tcp/0

```
    Path            : /usr/lib/jvm/java-11-openjdk-amd64/
    Version         : Unknown
    Binary Location : /usr/lib/jvm/java-11-openjdk-amd64/bin/java
    Managed by OS   : True
```

tcp/0

```
    Path            : /usr/lib/jvm/java-17-openjdk-amd64/
    Version         : Unknown
    Binary Location : /usr/lib/jvm/java-17-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.

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2024/01/16

Plugin Output

tcp/0

```
Nessus detected 7 installs of OpenSSL:

  Path               : /opt/nessus/bin/openssl
  Version            : 3.0.12
  Associated Package : nessus

  Path               : /usr/lib/x86_64-linux-gnu/ruby/3.1.0/openssl.so
  Version            : 3.1.4
  Associated Package : libruby3.1

  Path               : /usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Version            : 3.1.4
  Associated Package : libssl3

  Path    : /opt/lampp/lib/libcrypto.so.1.1
  Version : 1.1.1w
```

```
  Path             : /usr/bin/openssl
  Version          : 3.1.4
  Associated Package : openssl 3.1.4-2
  Managed by OS    : True


  Path    : /opt/lampp/lib/libssl.so.1.1
  Version : 1.1.1w


  Path    : /opt/lampp/bin/openssl
  Version : 1.1.1w

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
```

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: 2024/01/16

Plugin Output

tcp/0

```
 . You need to take the following 3 actions :

 [ Curl 7.46.0 <= 8.4.0 Information Disclosure (CVE-2023-46218) (187725) ]

 + Action to take : Upgrade Curl to version 8.5.0 or later


 [ OpenSSL 1.1.1 < 1.1.1x Vulnerability (184811) ]

 + Action to take : Upgrade to OpenSSL version 1.1.1x or later.


 [ libcurl 7.9.1 < 8.4.0 Cookie Injection (182873) ]

 + Action to take : Upgrade libcurl to version 8.4.0 or later
```

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: 2024/01/16

Plugin Output

tcp/0

```
 Path    : /usr/lib/postgresql/16/bin/postgres/usr/lib/postgresql/16/lib/bitcode/postgres
(via package manager)
 Version : 16.1
```

tcp/0

```
 Path    : /usr/lib/postgresql/16/bin/psql (via package manager)
 Version : 16.1
```

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

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

Solution

Disable IPv6 if you do not actually using it.

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
The following global addresss were gathered :

  - ['ipv6': ::1]['scope': host]['scopeid': 0x10]['prefixlen': 128]
  - ['ipv6': fe80::245:e2ff:fe55:386b]['scope': link]['scopeid': 0x20]['prefixlen': 64]
```

133964 - SELinux Status Check

Synopsis

SELinux is available on the host and plugin was able to check if it is enabled.

Description

SELinux is available on the host and plugin was able to check if it is enabled.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/02/25, Modified: 2024/01/16

Plugin Output

tcp/0

```
SELinux config has been found on the host.

SELinux is enabled.
SELinux policy: default.
SELinux status: permissive.
```

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: 2024/01/16

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 81 F7

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 27 05:57:23 2024 GMT
Not Valid After: Jan 26 05:57:23 2028 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 9C F6 F2 04 20 32 FE 86 33 35 40 C6 6C 79 34 50 A7 79 8F
```

```
          9C 2B 6A 30 B3 BD 82 B7 07 0C 32 97 C6 44 B0 6D 7B 47 D0 60
          C5 F2 ED 35 8B 6E AA 86 4D C6 D3 58 D4 53 01 99 96 DC 1A F2
          EC 0A E6 53 89 81 D4 86 A7 88 B5 FE AE 3C C0 80 B4 89 1E 91
          E2 88 19 56 08 10 6D CA 16 3E 59 DA 04 3F 18 17 0C 01 8D B7
          72 87 27 D6 94 C9 36 AE 7C 02 33 97 5C 9F 79 44 76 18 B3 B2
          3C 91 3F 35 B4 76 BD B8 EE 84 BD C0 1C 0E 26 0C B3 15 EE 6D
          2D 3B BA 2D A3 E1 28 54 22 FC 47 0A 3B D1 CC F8 D9 4C 35 2F
          56 87 3B B4 3B B8 53 B1 0E 76 14 7B 41 39 27 2E 0A 90 58 72
          9E E9 63 65 E4 91 19 FF E3 34 D6 00 EE 0B 02 09 02 3F 56 0E
          C7 77 13 53 D9 22 FE 28 D6 6F 91 DC 8E 59 59 70 E2 D1 55 95
          32 55 1B 10 CE 87 55 AE AB 94 A2 65 AE FF AE 60 69 DB B6 24
          C5 38 92 8A 68 D8 6E E7 58 B0 46 01 8C 5F A6 E7 27
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 20 E7 D6 D4 6A 4C A9 CA F5 AA 90 CE F6 A7 C0 32 0A 52 BA
          D2 0F B4 4C 50 CD B4 BE 66 0E 3E 28 F6 AF E4 90 53 BF 85 F3
          95 44 E7 BB D9 83 59 92 52 D9 9A 28 69 C6 C5 F6 D1 28 D3 FC
          C1 EB EE A0 D5 DF 3C 31 82 3C 82 A2 5F A0 36 2B A4 73 A5 61
          72 F4 17 AA 02 B9 F6 12 C7 3E 6A C6 84 1B E6 E5 D7 AB E3 7F
          D1 32 2D 28 F3 87 3E 50 6D E3 48 3E 46 81 09 78 28 D2 AE E4
          A9 45 E7 9F 77 01  [...]
```

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: 2023/07/10

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

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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 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: 2023/07/10

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.
```

22869 - Software Enumeration (SSH)

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, qpkg, 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: 2022/09/06

Plugin Output

tcp/0

```
 Here is the list of packages installed on the remote Debian Linux system :

   ii   accountsservice  23.13.9-5+b1  amd64  query and manipulate user account information
   ii   acl  2.3.1-4  amd64  access control list - utilities
   ii   adduser  3.137  all  add and remove users and groups
   ii   adwaita-icon-theme  45.0-2  all  default icon theme of GNOME
   ii   aircrack-ng  1:1.7-5  amd64  wireless WEP/WPA cracking utilities
   ii   airgeddon  11.21+ds-0kali1  amd64  multi-use bash script for Linux systems to audit wireless
  networks
   ii   alsa-topology-conf  1.2.5.1-2  all  ALSA topology configuration files
   ii   alsa-ucm-conf  1.2.10-1  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  3.20231019.1  amd64  Processor microcode firmware for AMD CPUs
   ii   apache2  2.4.58-1+b1  amd64  Apache HTTP Server
   ii   apache2-bin  2.4.58-1+b1  amd64  Apache HTTP Server (modules and other binary files)
   ii   apache2-data  2.4.58-1  all  Apache HTTP Server (common files)
   ii   apache2-utils  2.4.58-1+b1  amd64  Apache HTTP Server (utility programs for web servers)
   ii   apparmor  3.0.12-1+b2  amd64  user-space parser utility for AppArmor
   ii   apt  2.7.6  amd64  commandline package manager
   ii   apt-file  3.3  all  search for files within Debian packages (command-line interface)
   ii   apt-utils  2.7.6  amd64  package management related utility programs
```

```
ii   arj  3.10.22-26  amd64  archiver for .arj files
ii   arp-scan  1.10.0-2  amd64  arp scanning and fingerprinting tool
ii   arping  2.23-1  amd64  sends IP and/or ARP pings (to the MAC address)
ii   asleap  2.3~git20201128.254acab-0kali1  amd64  A tool for exploiting Cisco LEAP networks
ii   aspell  0.60.8.1-1+b1  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   asp [...]
```

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: 2024/01/22

Plugin Output

tcp/0

```
Nessus was able to execute commands locally with sufficient privileges
for all planned checks.
```

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: 2024/01/22

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: 2024/01/16

Plugin Output

tcp/0

```
Path    : /opt/nessus
Version : 10.6.4
Build   : 20005
```

56468 - Time of Last System Startup

Synopsis

The system has been started.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 29 03:34    still running
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 29 02:50 - 03:33   (00:43)
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 29 01:56 - 02:10   (00:14)
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 29 00:00 - 01:55   (01:54)
  reboot   system boot  6.5.0-kali3-amd6 Sun Jan 28 23:36 - 23:43   (00:07)
  reboot   system boot  6.5.0-kali3-amd6 Sun Jan 28 09:58 - 10:05   (00:07)
  reboot   system boot  6.5.0-kali3-amd6 Sat Jan 27 07:44 - 08:39   (00:54)
  reboot   system boot  6.5.0-kali3-amd6 Thu Jan 25 12:43 - 13:10   (00:27)
  reboot   system boot  6.5.0-kali3-amd6 Thu Jan 25 12:38 - 13:10   (00:32)
  reboot   system boot  6.5.0-kali3-amd6 Wed Jan 24 14:44 - 16:58   (02:13)
  reboot   system boot  6.5.0-kali3-amd6 Wed Jan 24 12:00 - 12:20   (00:20)
  reboot   system boot  6.5.0-kali3-amd6 Wed Jan 24 09:45 - 09:57   (00:12)
  reboot   system boot  6.5.0-kali3-amd6 Fri Jan 19 06:38 - 06:42   (00:04)
  reboot   system boot  6.5.0-kali3-amd6 Thu Jan 18 21:52 - 23:10   (01:18)
  reboot   system boot  6.5.0-kali3-amd6 Wed Jan 17 08:19 - 02:03   (17:44)
  reboot   system boot  6.5.0-kali3-amd6 Tue Jan 16 21:43 - 22:38   (00:55)
  reboot   system boot  6.5.0-kali3-amd6 Tue Jan 16 20:36 - 20:57   (00:20)
  reboot   system boot  6.5.0-kali3-amd6 Tue Jan 16 18:45 - 18:47   (00:02)
  reboot   system boot  6.5.0-kali3-amd6 Tue Jan 16 16:36 - 17:49   (01:13)
  reboot   system boot  6.5.0-kali3-amd6 Tue Jan 16 07:29 - 12:33   (05:04)
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 15 23:16 - 23:18   (00:02)
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 15 23:09 - 23:16   (00:07)
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 15 17:00 - 19:35   (02:35)
  reboot   system boot  6.5.0-kali3-amd6 Mon Jan 15 10:02 - 12:55   (02:52)
  reboot   system boot  6.5.0-kali3-amd6 Sun Jan 14 10:11 - 12:55 (1+02:43)
  reboot   system boot  6.5.0-kali3-amd6 Sun Jan 14 08:51 - 09:44   (00:53)
  reboot   system boot  6.5.0-kali3-amd6 Sat Jan 13 19:12 - 21:23   (02:10)
  reboot   system boot  [...]
```

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  0.0  0.3  22320  12652 ?        Ss   03:34   0:01 /sbin/init splash
root            2  0.0  0.0      0      0 ?        S    03:34   0:00 [kthreadd]
root            3  0.0  0.0      0      0 ?        I<   03:34   0:00 [rcu_gp]
root            4  0.0  0.0      0      0 ?        I<   03:34   0:00 [rcu_par_gp]
root            5  0.0  0.0      0      0 ?        I<   03:34   0:00 [slub_flushwq]
root            6  0.0  0.0      0      0 ?        I<   03:34   0:00 [netns]
root            7  0.0  0.0      0      0 ?        I    03:34   0:00 [kworker/0:0-i915-unordered]
root            8  0.0  0.0      0      0 ?        I<   03:34   0:00 [kworker/0:0H-events_highpri]
root           11  0.0  0.0      0      0 ?        I<   03:34   0:00 [mm_percpu_wq]
root           12  0.0  0.0      0      0 ?        I    03:34   0:00 [rcu_tasks_kthread]
root           13  0.0  0.0      0      0 ?        I    03:34   0:00 [rcu_tasks_rude_kthread]
root           14  0.0  0.0      0      0 ?        I    03:34   0:00 [rcu_tasks_trace_kthread]
root           15  0.0  0.0      0      0 ?        S    03:34   0:00 [ksoftirqd/0]
root           16  0.0  0.0      0      0 ?        I    03:34   0:00 [rcu_preempt]
root           17  0.0  0.0      0      0 ?        S    03:34   0:00 [migration/0]
root           18  0.0  0.0      0      0 ?        S    03:34   0:00 [idle_inject/0]
root           19  0.0  0.0      0      0 ?        S    03:34   0:00 [cpuhp/0]
root           20  0.0  0.0      0      0 ?        S    03:34   0:00 [cpuhp/1]
root           21  0.0  0.0      0      0 ?        S    03:34   0:00 [idle_inject/1]
root           22  0.0  0.0      0      0 ?        S    03:34   0:00 [migration/1]
root           23  0.0  0.0      0      0 ?        S    03:34   0:00 [ksoftirqd/1]
root           25  0.0  0.0      0      0 ?        I<   03:34   0:00 [kworker/1:0H-events_highpri]
root           26  0.0  0.0      0      0 ?        S    03:34   0:00 [cpuhp/2]
root           27  0.0  0.0      0      0 ?        S    [...]
```

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
```

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.

Note that more paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2024/01/16

Plugin Output

tcp/0

```
Nessus detected 3 installs of libcurl:

  Path              : /usr/lib/x86_64-linux-gnu/libcurl.so.4.8.0
  Version           : 8.5.0
  Associated Package : libcurl4 8.5.0-2
  Managed by OS     : True

  Path              : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.8.0
  Version           : 8.5.0
  Associated Package : libcurl3-gnutls 8.5.0-2
  Managed by OS     : True

  Path    : /opt/lampp/lib/libcurl.so.4.4.0
  Version : 7.53.1
```

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: 2024/01/16

Plugin Output

tcp/0

```
Path             : /usr/sbin/nginx
Version          : 1.24.0
Detection Method : Binary in $PATH
Full Version     : 1.24.0
Nginx Plus       : False
```