vuln scan

Report generated by Nessus™ Mon, 18 Dec 2023 21:27:35 IST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.0.104

0	0	0	0	4
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Dec 18 21:10:59 2023
End time:	Mon Dec 18 21:23:34 2023

Host Information

IP:	192.168.0.104
MAC Address:	B0:35:9F:F6:1B:25

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

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

Plugin Output

tcp/0

```
The following card manufacturers were identified :

B0:35:9F:F6:1B:25 : 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:
  - B0:35:9F:F6:1B:25
```

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- Whether the display of superseded patches is enabled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 : 202312180003
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : vuln scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.108
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 236.643 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 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 : 2023/12/18 21:11 IST
Scan duration : 745 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 192.168.0.108 to 192.168.0.104 :
192.168.0.108

ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

192.168.0.108

0	1	1	0	59
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Mon Dec 18 21:10:59 2023
End time:	Mon Dec 18 21:27:35 2023

Host Information

IP:	192.168.0.108
MAC Address:	40:ED:00:30:E2:CF 00:0C:29:A4:8C:B8
OS:	Linux Kernel 6.1.0-kali9-amd64

Vulnerabilities

174697 - OpenJDK 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <= 20.0.0 Multiple Vulnerabilities (2023-04-18

Synopsis

OpenJDK is affected by multiple vulnerabilities.

Description

The version of OpenJDK installed on the remote host is prior to 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <= 20.0.0. It is, therefore, affected by multiple vulnerabilities as referenced in the 2023-04-18 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 Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability 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. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2023-21930)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability 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. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2023-21954)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability 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. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2023-21967)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, 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 Enterprise Edition accessible data. Note: This vulnerability 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. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.

(CVE-2023-21939)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, 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 Enterprise Edition accessible data. Note: This vulnerability 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. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). (CVE-2023-21938)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, 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 Enterprise Edition accessible data. Note: This vulnerability 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. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2023-21937)

- Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, 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 Enterprise Edition accessible data. Note: This vulnerability 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. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. (CVE-2023-21968)

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://openjdk.java.net/groups/vulnerability/advisories/2023-04-18

Solution

Upgrade to an OpenJDK version greater than 8u362 / 11.0.18 / 17.0.6 / 20.0.0

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-21930
CVE	CVE-2023-21937
CVE	CVE-2023-21938
CVE	CVE-2023-21939
CVE	CVE-2023-21954
CVE	CVE-2023-21967
CVE	CVE-2023-21968

Plugin Information

Published: 2023/04/25, Modified: 2023/04/25

Plugin Output

tcp/0

```
  Path              : /usr/lib/jvm/java-17-openjdk-amd64/
  Installed version : 17.0.6
  Fixed version     : Upgrade to a version greater than 17.0.6
```

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: 2023/12/14

Plugin Output

tcp/0

```
Path               : /usr/sbin/apache2
Version            : 2.4.55
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: 2023/10/16

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: 2023/10/16

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:2.4.55 -> Apache Software Foundation Apache HTTP Server
  cpe:/a:gnupg:libgcrypt:1.10.1 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.87.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.87.0 -> Haxx libcurl
  cpe:/a:nginx:nginx:1.22.1 -> Nginx
  cpe:/a:openssl:openssl:3.0.12 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:3.0.8 -> OpenSSL Project OpenSSL
  cpe:/a:oracle:openjdk:1.17.0_6 -> Oracle OpenJDK -
  cpe:/a:postgresql:postgresql:15.2 -> PostgreSQL
  cpe:/a:sqlite:sqlite -> SQLite
  cpe:/a:tenable:nessus -> Tenable Nessus
  cpe:/a:tenable:nessus:10.6.4 -> Tenable Nessus
```

```
    cpe:/a:vmware:open_vm_tools:12.1.5
    x-cpe:/a:java:jre:1.17.0_6
```

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: 2023/12/14

Plugin Output

tcp/0

```
  Path               : /usr/bin/curl
  Version            : 7.87.0
  Associated Package : curl 7.87.0-2
  Managed by OS      : True
```

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: 2023/12/14

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: 2023/11/14

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: 2023/12/14

Plugin Output

tcp/0

```
Dockerfiles found: 4
 - /usr/share/king-phisher/tools/mac_client/Dockerfile
 - /usr/share/metasploit-framework/tools/payloads/ysoserial/Dockerfile
 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/net-ssh-7.0.1/Dockerfile
 - /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/puma-6.1.0/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)
 - 192.168.0.108 (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::e83f:9724:fd6a:6fe9 (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 addresses exist on the remote host :

  - 40:ed:00:30:e2:cf (interface wlan0)
  - 00:0c:29:a4:8c:b8 (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: 2023/11/17

Plugin Output

tcp/0

```
wlan0:
  MAC : 40:ed:00:30:e2:cf
  IPv4:
    - Address : 192.168.0.108
        Netmask : 255.255.255.0
        Broadcast : 192.168.0.255
  IPv6:
    - Address : fe80::e83f:9724:fd6a:6fe9
        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
eth0:
  MAC : 00:0c:29:a4:8c:b8
```

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:
      192.168.0.1:
        subnets:
          - 0.0.0.0/0
Interface Routes:
  wlan0:
    ipv4_subnets:
      - 192.168.0.0/24
    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: 2023/12/14

Plugin Output

tcp/0

```
Nessus has enumerated the path of the current scan user :

/usr/local/sbin
/usr/local/bin
/usr/sbin
/usr/bin
/sbin
/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 :

40:ED:00:30:E2:CF : TP-Link Corporation Limited
00:0C:29:A4:8C:B8 : 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:
  - 40:ED:00:30:E2:CF
  - 00:0C:29:A4:8C:B8
```

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:

/root/node_modules/@azure/identity/package.json
```

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, 18 Dec 2023 15:41:30 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=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: 2023/12/14

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address        : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address        : ::1
      Assign Method : static
+ eth0
+ wlan0
  + IPv4
    - Address        : 192.168.0.108
      Assign Method : dynamic
  + IPv6
    - Address        : fe80::e83f:9724:fd6a:6fe9
      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: 2023/12/14

Plugin Output

tcp/0

```
  Path             : /usr/lib/jvm/java-17-openjdk-amd64/
  Version          : 1.17.0_6
  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: 2023/12/14

Plugin Output

tcp/0

```
Nessus detected 4 installs of Libgcrypt:

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.4.1
  Version : 1.10.1

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.10.1

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.4.1
  Version : 1.10.1

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.10.1
```

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            929M     0  929M   0% /dev
tmpfs           194M  1.2M  193M   1% /run
/dev/sda1        29G   20G  7.6G  72% /
tmpfs           967M     0  967M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           194M   80K  194M   1% /run/user/1000


$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0   30G  0 disk
##sda1   8:1    0   29G  0 part /
##sda2   8:2    0    1K  0 part
##sda5   8:5    0  975M  0 part [SWAP]
sr0     11:0    1  3.6G  0 rom


$ 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=950700k,nr_inodes=237675,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=197908k,mode=755,inode64)
```

```
/dev/sda1 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)
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=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=17130)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (r [...]
```

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         : abhinavlather
Home folder  : /home/abhinavlather
Start script : /usr/bin/zsh
Groups       : dip
               scanner
               netdev
               users
               dialout
               wireshark
               video
               cdrom
               abhinavlather
               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: 2023/07/31

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.6.4
Nessus build : 20005
Plugin feed version : 202312180003
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1404-x86-64
Scan type : Normal
Scan name : vuln scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.0.108
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 : 2023/12/18 21:10 IST
Scan duration : 994 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://192.168.0.108:8834/
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: 2023/11/24

Plugin Output

tcp/8834/www

```
Port 8834/tcp was found to be open
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2023/11/08

Plugin Output

tcp/0

```

Remote operating system : Linux Kernel 6.1.0-kali9-amd64
Confidence level : 99
Method : uname


The remote host is running Linux Kernel 6.1.0-kali9-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 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) 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 : 1.847453 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: 2023/10/16

Plugin Output

tcp/0

```
  Path            : /usr/lib/jvm/java-17-openjdk-amd64/
  Version         : 1.17.0_6
  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.

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2023/12/14

Plugin Output

tcp/0

```
Nessus detected 2 installs of OpenSSL:

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

  Path    : /usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Version : 3.0.8

We are unable to retrieve version info from the following list of OpenSSL files. However, they may
 include their OpenSSL version in full or part at the end of their names.

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
/usr/share/bash-completion/completions/openssl
```

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: 2023/12/12

Plugin Output

tcp/0

```
. You need to take the following action :

[ OpenJDK 8 <= 8u362 / 11.0.0 <= 11.0.18 / 17.0.0 <= 17.0.6 / 20.0.0 <= 20.0.0 Multiple
 Vulnerabilities (2023-04-18 (174697) ]

+ Action to take : Upgrade to an OpenJDK version greater than 8u362 / 11.0.18 / 17.0.6 / 20.0.0
```

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: 2023/12/14

Plugin Output

tcp/0

```
 Path    : /usr/lib/postgresql/15/bin/postgres/usr/lib/postgresql/15/lib/bitcode/postgres
(via package manager)
 Version : 15.2
```

tcp/0

```
 Path    : /usr/lib/postgresql/15/bin/psql (via package manager)
 Version : 15.2
```

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::e83f:9724:fd6a:6fe9]['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: 2023/12/14

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: 2023/12/14

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 EA A5

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Dec 18 05:31:32 2023 GMT
Not Valid After: Dec 17 05:31:32 2027 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 D1 4F A2 E5 09 C8 44 67 77 36 D6 20 71 47 63 D7 A9 D6 98
```

```
            9C E0 4F 74 C8 1D 49 72 37 E8 E8 B8 DC 19 70 74 7A D7 26 08
            F7 30 0E EF E8 F8 79 F9 3E 48 1E 52 DE 75 4C EA 79 F2 2B 58
            6E FF 78 56 43 67 69 32 20 2F 54 CA D3 0E DE 95 00 C4 B8 EB
            AE AC BA EF 17 FB 24 3F C7 3A 21 7D 67 0C 91 DF 2A A4 28 49
            2D 94 8D 35 AE E4 52 28 26 56 97 21 33 76 E7 0A 72 2F 50 2C
            1D C5 EE B4 98 9F 10 90 7A 63 EA 05 79 45 43 61 61 EF 35 C4
            21 5A E6 07 96 D2 95 AE 3B 34 C7 95 68 75 9B 97 03 FB F4 8B
            EA 93 9A E9 C5 BD CB 16 2D 54 41 10 99 A7 74 E1 9D 3F 5F 1D
            1D 79 A6 D7 B1 8C 83 8A D1 23 F6 73 AA 44 DC 39 71 9A DE A5
            64 29 DE C2 1D 0D 26 89 03 7C 20 86 1F 73 DE F2 2E 3E EF 80
            1F 03 4E FE A7 57 FC 4A 4A 11 A8 88 0D CE 97 DD D3 92 3E B1
            1E 2D 9A 86 71 32 CD 95 83 C8 2C F1 60 BE E9 E2 6B
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 1C 9C 5D 03 4A 75 72 51 1E D5 B5 22 A6 9D 52 A0 10 D5 12
           8F 8C 78 3D E1 B7 24 5A F8 28 B6 74 BA 6C E2 14 EB 38 62 FC
           BC BA 38 F7 30 D2 8E B9 AB BE 7B 50 45 E2 C6 37 6E B0 F0 E6
           0A 7E E6 FE E4 34 CB 1E 1E 4B 48 B6 D6 11 CC EE C1 D1 3C 67
           F9 08 7C 2A CE 3A B5 3C 4D 62 2F 21 B7 C5 74 94 74 3A CA E6
           E8 89 CF D1 08 DD 55 29 81 52 C5 87 B5 76 41 D1 C2 10 E1 B5
           A2 7B C8 96 46 68  [...]
```

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   acl  2.3.1-3  amd64  access control list - utilities
  ii   adduser  3.131  all  add and remove users and groups
  ii   adwaita-icon-theme  43-1  all  default icon theme of GNOME
  ii   aircrack-ng  1:1.7-5  amd64  wireless WEP/WPA cracking utilities
  ii   alien  8.95.6  all  convert and install rpm and other packages
  ii   alsa-topology-conf  1.2.5.1-2  all  ALSA topology configuration files
  ii   alsa-ucm-conf  1.2.8-1  all  ALSA Use Case Manager configuration files
  ii   amass  3.21.2-0kali1  amd64  In-depth DNS Enumeration and Network Mapping
  ii   amass-common  3.21.2-0kali1  all  In-depth DNS Enumeration and Network Mapping
  ii   amd64-microcode  3.20220411.2  amd64  Processor microcode firmware for AMD CPUs
  ii   apache2  2.4.55-1  amd64  Apache HTTP Server
  ii   apache2-bin  2.4.55-1  amd64  Apache HTTP Server (modules and other binary files)
  ii   apache2-data  2.4.55-1  all  Apache HTTP Server (common files)
  ii   apache2-utils  2.4.55-1  amd64  Apache HTTP Server (utility programs for web servers)
  ii   apparmor  3.0.8-3  amd64  user-space parser utility for AppArmor
  ii   apt  2.5.6  amd64  commandline package manager
  ii   apt-file  3.3  all  search for files within Debian packages (command-line interface)
  ii   apt-utils  2.5.6  amd64  package management related utility programs
  ii   aptitude  0.8.13-5  amd64  terminal-based package manager
```

```
 ii   aptitude-common  0.8.13-5  all  architecture independent files for the aptitude package
manager
 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   aspell  0.60.8-4+b1  amd64  GNU Aspell spell-checker
 ii   aspell-en  2018.04.16-0-1  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  2.46.0 [...]
```

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: 2021/07/26

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: 2021/07/26

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: 2023/12/14

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  6.1.0-kali9-amd6 Mon Dec 18 20:59   still running
reboot   system boot  6.1.0-kali9-amd6 Mon Dec 18 10:48   still running
reboot   system boot  6.1.0-kali9-amd6 Sat Oct 21 16:01 - 10:48 (57+18:46)
reboot   system boot  6.1.0-kali9-amd6 Sat Oct 21 15:32 - 16:01  (00:28)
reboot   system boot  6.1.0-kali9-amd6 Sat Oct 21 14:50 - 15:09  (00:18)
reboot   system boot  6.1.0-kali9-amd6 Thu Oct 19 11:40 - 14:58  (03:17)
reboot   system boot  6.1.0-kali9-amd6 Fri Oct 13 13:59 - 14:02 (3+00:02)
reboot   system boot  6.1.0-kali9-amd6 Mon Oct  9 12:01 - 12:50  (00:48)
reboot   system boot  6.1.0-kali9-amd6 Wed Sep 13 22:22 - 16:43 (9+18:20)
reboot   system boot  6.1.0-kali9-amd6 Wed Sep 13 18:01 - 18:18  (00:17)
reboot   system boot  6.1.0-kali9-amd6 Tue Sep  5 21:00 - 10:25 (3+13:25)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 31 11:47 - 15:34  (03:47)
reboot   system boot  6.1.0-kali9-amd6 Wed Aug 30 19:28 - 11:45  (16:17)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 17 17:38 - 14:43  (21:05)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 17 17:34 - 17:36  (00:02)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 17 17:18 - 17:32  (00:14)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 17 17:13 - 17:17  (00:03)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 17 16:56 - 17:12  (00:15)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 17 15:42 - 16:55  (01:13)
reboot   system boot  6.1.0-kali9-amd6 Thu Aug 10 17:22 - 17:23  (00:01)
reboot   system boot  6.1.0-kali9-amd6 Sat Jul 29 11:08 - 13:10  (02:01)
reboot   system boot  6.1.0-kali9-amd6 Thu Jul 27 11:20 - 12:35  (01:15)
reboot   system boot  6.1.0-kali9-amd6 Sun Jul 23 11:45 - 13:36 (3+01:51)
reboot   system boot  6.1.0-kali9-amd6 Thu Jul 20 15:37 - 16:40  (01:03)
reboot   system boot  6.1.0-kali9-amd6 Tue Jul 18 12:34 - 16:40 (2+04:06)
reboot   system boot  6.1.0-kali9-amd6 Tue Jul 18 11:18 - 16:40 (2+05:22)
reboot   system boot  6.1.0-kali9-amd6 Sun Jul 16 11:27 - 13:24  (01:57)
reboot   system [...]
```

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  0.3 102316  6600 ?        Ss   20:59   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    20:59   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   20:59   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   20:59   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   20:59   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   20:59   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   20:59   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   20:59   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    20:59   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    20:59   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    20:59   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    20:59   0:00 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    20:59   0:00 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    20:59   0:00 [migration/0]
root          17  0.1  0.0      0     0 ?        I    20:59   0:01 [kworker/0:1-events]
root          18  0.0  0.0      0     0 ?        S    20:59   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    20:59   0:00 [kdevtmpfs]
root          21  0.0  0.0      0     0 ?        I<   20:59   0:00 [inet_frag_wq]
root          22  0.0  0.0      0     0 ?        S    20:59   0:00 [kauditd]
root          23  0.1  0.0      0     0 ?        D    20:59   0:00 [kworker/0:2+usb_hub_wq]
root          24  0.0  0.0      0     0 ?        S    20:59   0:00 [khungtaskd]
root          25  0.0  0.0      0     0 ?        S    20:59   0:00 [oom_reaper]
root          26  0.0  0.0      0     0 ?        I    20:59   0:00 [kworker/u256:1-ext4-rsv-
conversion]
root          27  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: 2023/12/14

Plugin Output

tcp/0

```
  Path    : /usr/bin/vmtoolsd
  Version : 12.1.5
```

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.
```

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: 2023/12/14

Plugin Output

tcp/0

```

Nessus detected 3 installs of libcurl:

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.8.0
  Version            : 7.87.0
  Associated Package : libcurl4 7.87.0-2
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.8.0
  Version            : 7.87.0
  Associated Package : libcurl3-gnutls 7.87.0-2
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-nss.so.4.8.0
  Version            : 7.87.0
  Associated Package : libcurl3-nss 7.87.0-2
  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: 2023/12/14

Plugin Output

tcp/0

```
  Path             : /usr/sbin/nginx
  Version          : 1.22.1
  Detection Method : Binary in $PATH
  Full Version     : 1.22.1
  Nginx Plus       : False
```