my-scan-on-aws

Report generated by Tenable Nessus™ Sun, 20 Jul 2025 00:08:32 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

172.31.94.8

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	67

Scan Information

Start time: Thu Jul 17 14:39:17 2025
End time: Thu Jul 17 14:46:24 2025

Host Information

DNS Name: ip-172-31-94-8.ec2.internal
IP: 172.31.94.8
MAC Address: 12:0C:23:A2:7D:EF
OS: Linux Kernel 6.1.141-165.249.amzn2023.x86_64 on Amazon Linux 2023

Vulnerabilities

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2010/12/15, Modified: 2025/06/16

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=ip-172-31-94-8.ec2.internal
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```

212053 - Amazon Linux : Enabled Official Repositories and Extras

Synopsis

The remote host is using one or more Amazon Linux repositories to install packages.

Description

The remote host is using one or more Amazon Linux repositories to install packages.

These repositories may be used in conjuntion with Amazon Linux OS package level assessment security advisories to determine whether or not relevant repositories are installed before checking package versions for vulnerable ranges.

See Also

http://www.nessus.org/u?804d18c7

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/12/04, Modified: 2024/12/04

Plugin Output

tcp/0

```
Amazon Linux Repositories found to be enabled:
  amazonlinux
  kernel-livepatch
```

190682 - Amazon Systems Manager (SSM) Agent Installed (Linux)

Synopsis

Amazon Systems Manager (SSM) Agent is installed on the remote Linux host.

Description

Amazon Systems Manager (SSM) Agent is installed on the remote Linux host.

See Also

http://www.nessus.org/u?a0d6abc7

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/02/19, Modified: 2025/07/14

Plugin Output

tcp/0

```
Path    : amazon-ssm-agent (via package manager)
Version : 3.3.2299.0
Running : Yes
```

90191 - Amazon Web Services EC2 Instance Metadata Enumeration (Unix)

Synopsis

The remote host is an AWS EC2 instance for which metadata could be retrieved.

Description

The remote host appears to be an Amazon Machine Image. Nessus was able to use the metadata API to collect information about the system.

See Also

https://docs.aws.amazon.com/ec2/index.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/03/25, Modified: 2025/01/21

Plugin Output

tcp/0

```
It was possible to retrieve the following API items :

  - accountId: 556712931248
  - architecture: x86_64
  - availabilityZone: us-east-1b
  - billingProducts: null
  - devpayProductCodes: null
  - marketplaceProductCodes: null
  - imageId: ami-0150ccaf51ab55a51
  - instanceId: i-04a500c34fce21170
  - instanceType: t2.micro
  - kernelId: null
  - pendingTime: 2025-07-17T13:37:26Z
  - privateIp: 172.31.94.8
  - ramdiskId: null
  - region: us-east-1
  - version: 2017-09-30
  - instance-id: i-04a500c34fce21170
  - public-hostname: ec2-34-239-126-18.compute-1.amazonaws.com
  - hostname: ip-172-31-94-8.ec2.internal
  - local-ipv4: 172.31.94.8
  - local-hostname: ip-172-31-94-8.ec2.internal
  - public-ipv4: 34.239.126.18
```

```
    - ami-id: ami-0150ccaf51ab55a51
    - mac: 12:0c:23:a2:7d:ef
    - block-device-mapping-ami: /dev/xvda
    - block-device-mapping-root: /dev/xvda
    - block-device-mapping-ebs-count: 0
    - block-device-mapping-ephemeral-count: 0
    - vpc-id: vpc-0f5f688f1ba814bf0
```

34098 - BIOS Info (SSH)

Synopsis

BIOS info could be read.

Description

Using SMBIOS and UEFI, it was possible to get BIOS info.

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2008/09/08, Modified: 2024/02/12

Plugin Output

tcp/0

```
Version      : 4.11.amazon
Vendor       : Xen
Release Date : 08/24/2006
UUID         : ec2c1413-df11-b49e-ba9a-4955fe6c7626
Secure boot  : disabled
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

```
Local checks have been enabled.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2025/07/14

Plugin Output

tcp/0

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

  cpe:/o:amazon:linux_2:2023.8.20250707::~~~~x86_64~ -> Amazon Linux 2

Following application CPE's matched on the remote system :

  cpe:/a:amazon:amazon_ssm_agent:3.3.2299.0 -> Amazon SSM Agent
  cpe:/a:gnupg:libgcrypt:1.10.2 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:8.11.1 -> Haxx Curl
  cpe:/a:haxx:libcurl:8.11.1 -> Haxx libcurl
  cpe:/a:openbsd:openssh:8.7 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:3.0.16 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:3.2.2 -> OpenSSL Project OpenSSL
  cpe:/a:tenable:nessus -> Tenable Nessus
  cpe:/a:tenable:nessus:10.9.1 -> Tenable Nessus
  cpe:/a:tukaani:xz:5.2.5 -> Tukaani XZ
  cpe:/a:vim:vim:9.1 -> Vim
```

182774 - Curl Installed (Linux / Unix)

Synopsis

Curl is installed on the remote Linux / Unix host.

Description

Curl (also known as curl and cURL) is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182774' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/09, Modified: 2025/07/14

Plugin Output

tcp/0

```
Path               : /usr/bin/curl
Version            : 8.11.1
Associated Package : curl-minimal-8.11.1-4.amzn2023.0.1.x86_64
```

55472 - Device Hostname

Synopsis

It was possible to determine the remote system hostname.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/06/30, Modified: 2025/07/14

Plugin Output

tcp/0

```
Hostname : ip-172-31-94-8.ec2.internal
  ip-172-31-94-8.ec2.internal (hostname command)
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 100
```

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: 2025/04/28

Plugin Output

tcp/0

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

 - 172.31.94.8
 - 127.0.0.1 (on interface lo)
```

25202 - Enumerate IPv6 Interfaces via SSH

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2007/05/11, Modified: 2025/04/28

Plugin Output

tcp/0

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

 - fe80::100c:23ff:fea2:7def
 - ::1 (on interface lo)
```

170170 - Enumerate the Network Interface configuration via SSH

Synopsis

Nessus was able to parse the Network Interface data on the remote host.

Description

Nessus was able to parse the Network Interface data on the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/01/19, Modified: 2025/02/11

Plugin Output

tcp/0

```
lo:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
        Scope : host
        ScopeID : 0x10
enx0:
  MAC : 12:0c:23:a2:7d:ef
  IPv4:
    - Address : 172.31.94.8
        Netmask : 255.255.240.0
        Broadcast : 172.31.95.255
  IPv6:
    - Address : fe80::100c:23ff:fea2:7def
        Prefixlen : 64
        Scope : link
        ScopeID : 0x20
```

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:
  enX0:
    ipv4_gateways:
      172.31.80.1:
        subnets:
         - 0.0.0.0/0
Interface Routes:
  enX0:
    ipv4_subnets:
     - 172.31.80.0/20
    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: 2025/07/14

Plugin Output

tcp/0

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

/usr/local/sbin
/usr/local/bin
/usr/sbin
/usr/bin
```

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: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 12:0C:23:A2:7D:EF
```

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
```

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/02/11, Modified: 2025/03/13

Plugin Output

tcp/0

```
172.31.94.8 resolves as ip-172-31-94-8.ec2.internal.
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/8834/www

```
Response Code : HTTP/1.1 200 OK

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

  Cache-Control: must-revalidate
  X-Frame-Options: DENY
  Content-Type: text/html
  ETag: 40922806a299e780871ba3ee0874e013
  Connection: close
  X-XSS-Protection: 1; mode=block
  Server: NessusWWW
  Date: Thu, 17 Jul 2025 14:39:35 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; includeSubDomains
  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=1751916535202" id="theme-link" />
        <link rel="stylesheet" href="tenable_links.css?v=ac05d80f1e3731b79d12103cdf9367fc" />
        <link rel="stylesheet" href="wizard_templates.css?v=0e2ae10949ed6782467b3810ccce69c5" />
        <!--[if lt IE 11]>
            <script>
                window.location = '/unsupported6.html';
            </script>
        <![endif]-->
        <script src="nessus6.js?v=1751916535202"></script>
        <script src="pe [...]
```

171410 - IP Assignment Method Detection

Synopsis

Enumerates the IP address assignment method(static/dynamic).

Description

Enumerates the IP address assignment method(static/dynamic).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/02/14, Modified: 2025/07/14

Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ enX0
  + IPv4
    - Address       : 172.31.94.8
      Assign Method : dynamic
  + IPv6
    - Address       : fe80::100c:23ff:fea2:7def
      Assign Method : static
```

151883 - Libgcrypt Installed (Linux/UNIX)

Synopsis

Libgcrypt is installed on this host.

Description

Libgcrypt, a cryptography library, was found on the remote host.

See Also

https://gnupg.org/download/index.html

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/07/21, Modified: 2025/07/14

Plugin Output

tcp/0

```
Nessus detected 2 installs of Libgcrypt:

  Path    : /usr/lib64/libgcrypt.so.20
  Version : 1.10.2

  Path    : /usr/lib64/libgcrypt.so.20.4.2
  Version : 1.10.2
```

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
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           475M     0  475M   0% /dev/shm
tmpfs           190M  428K  190M   1% /run
/dev/xvda1       25G  9.1G   16G  37% /
tmpfs           475M     0  475M   0% /tmp
/dev/xvda128     10M  1.3M  8.7M  13% /boot/efi


$ lsblk
NAME      MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
xvda      202:0    0  25G  0 disk
├─xvda1   202:1    0  25G  0 part /
├─xvda127 259:0    0   1M  0 part
└─xvda128 259:1    0  10M  0 part /boot/efi


$ mount -l
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime,seclabel)
devtmpfs on /dev type devtmpfs (rw,nosuid,seclabel,size=4096k,nr_inodes=118532,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,seclabel)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,seclabel,gid=5,mode=620,ptmxmode=000)
```

```
tmpfs on /run type tmpfs (rw,nosuid,nodev,seclabel,size=194436k,nr_inodes=819200,mode=755)
cgroup2 on /sys/fs/cgroup type cgroup2
 (rw,nosuid,nodev,noexec,relatime,seclabel,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime,seclabel)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
/dev/xvda1 on / type xfs
 (rw,noatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,sunit=1024,swidth=1024,noquota) [/]
selinuxfs on /sys/fs/selinux type selinuxfs (rw,nosuid,noexec,relatime)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
 (rw,relatime,fd=33,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=13204)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime,seclabel)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,seclabel,pagesize=2M)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime,seclabel)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime,seclabel)
tmpfs on /tmp type tmpfs (rw,nosuid,node [...]
```

193143 - Linux Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Linux host.

Solution

None

Risk Factor

None

Plugin Information

Published: 2024/04/10, Modified: 2024/04/10

Plugin Output

tcp/0

```
Via date: UTC +0000
Via timedatectl: Time zone: n/a (UTC, +0000)
Via /etc/localtime: UTC0
```

95928 - Linux User List Enumeration

Synopsis

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

Description

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

Solution

None

Risk Factor

None

Plugin Information

Published: 2016/12/19, Modified: 2025/03/26

Plugin Output

tcp/0

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

User         : ec2-user
Home folder  : /home/ec2-user
Start script : /bin/bash
Groups       : systemd-journal
               ec2-user
               wheel
               adm

----------[ System Accounts ]----------

User         : root
Home folder  : /root
Start script : /bin/bash
Groups       : root

User         : bin
Home folder  : /bin
Start script : /sbin/nologin
Groups       : bin

User         : daemon
Home folder  : /sbin
Start script : /sbin/nologin
Groups       : daemon

User         : adm
Home folder  : /var/adm
```

```
Start script : /sbin/nologin
Groups       : adm

User         : lp
Home folder  : /var/spool/lpd
Start script : /sbin/nologin
Groups       : lp

User         : sync
Home folder  : /sbin
Start script : /bin/sync
Groups       : root

User         : shutdown
Home folder  : /sbin
Start script : /sbin/shutdown
Groups       : root

User         : halt
Home folder  : /sbin
Start script : /sbin/halt
Groups       : root

User         : mail
Home folder  : /var/spool/mail
Start script : /sbin/nologin
Groups       : mail

User         : operator
Home folder  : /root
Start script : /sbin/nologin
Groups       : root

User         : games
Home folder  : /usr/games
Start script : /sbin/nologin
Groups       : users

User         : ftp
Home folder  : /var/ftp
Start script : /sbin/nologin
Groups       : ftp

User         : nobody
Home folder  : /
Start script : /sbin/nologin
Groups       : nobody

User         : dbus
Home folder  : /
Start script : /sbin/nologin
Groups       : dbus

User         : systemd-network
Home folder  : /
Start script : /usr/sbin/nologin
Groups       : systemd-network

User         : systemd-oom
Home folder  : /
Start script : /usr/sbin/nologin
Groups       : systemd-oom

User         : systemd-resolve
Home folder  : /
Start script : /usr/sbin/nologin
Groups       : systemd-resolve

User         : sshd
Home folder  : /usr/share/empty.sshd
```

```
Start script : /sbin/nologin
Groups       : sshd

User         : rpc
Home folder  : /var/lib/rpcbind
Start scr [...]
```

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: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.1
Nessus build : 20006
Plugin feed version : 202507170221
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : es9-x86-64
Scan type : Normal
Scan name : my-scan-on-aws
```

```
Scan policy used : Advanced Scan
Scanner IP : 172.31.94.8
Ping RTT : Unavailable
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes (on the localhost)
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/7/17 14:39 UTC
Scan duration : 423 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://ip-172-31-94-8.ec2.internal: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

174736 - Netstat Ingress Connections

Synopsis

External connections are enumerated via the 'netstat' command.

Description

This plugin runs 'netstat' to enumerate any non-private connections to the scan target.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/04/25, Modified: 2025/07/14

Plugin Output

tcp/0

```
Netstat output indicated the following connections from non-private IP addresses:

92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.
92.72.49.215 connected to port 8834 on the scan target.

NOTE: This list may be truncated depending on the scan verbosity settings.
```

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/22/ssh

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/68

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

udp/546

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

14272 - Netstat Portscanner (SSH)

Synopsis

Remote open ports can be enumerated via SSH.

Description

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

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/08/15, Modified: 2025/05/27

Plugin Output

tcp/8834/www

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

209654 - OS Fingerprints Detected

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Linux Kernel 6.1.141-165.249.amzn2023.x86_64 on Amazon Linux 2023
Confidence level : 100
Method : uname
Type : general-purpose
Fingerprint : uname:Linux ip-172-31-94-8.ec2.internal 6.1.141-165.249.amzn2023.x86_64 #1 SMP
 PREEMPT_DYNAMIC Tue Jul  1 18:01:09 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux


Following fingerprints could not be used to determine OS :
 SSH:!:SSH-2.0-OpenSSH_8.7
HTTP:!:Server: NessusWWW

SSLcert:!:i/CN:Nessus Certification Authorityi/O:Nessus Users Unitedi/OU:Nessus Certification
 Authoritys/CN:ip-172-31-94-8.ec2.internals/O:Nessus Users Uniteds/OU:Nessus Server
536d277c423de8464fb6dd1c86728fe364ac165b
```

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: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 6.1.141-165.249.amzn2023.x86_64 on Amazon Linux 2023
Confidence level : 100
Method : uname


The remote host is running Linux Kernel 6.1.141-165.249.amzn2023.x86_64 on Amazon Linux 2023
```

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

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/05/30, Modified: 2025/02/11

Plugin Output

tcp/0

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

The output of "uname -a" is :
Linux ip-172-31-94-8.ec2.internal 6.1.141-165.249.amzn2023.x86_64 #1 SMP PREEMPT_DYNAMIC Tue Jul  1
 18:01:09 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Amazon Linux AMI system is :
Amazon Linux release 2023.8.20250707 (Amazon Linux)

OS Security Patch Assessment is available for this host.
Runtime : 1.796646 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
```

181418 - OpenSSH Detection

Synopsis

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

Description

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

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/07/14

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.7
Banner  : SSH-2.0-OpenSSH_8.7
```

168007 - OpenSSL Installed (Linux)

Synopsis

OpenSSL was detected on the remote Linux host.

Description

OpenSSL was detected on the remote Linux host.

The plugin timeout can be set to a custom value other than the plugin's default of 15 minutes via the 'timeout.168007' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

Note: This plugin leverages the '-maxdepth' find command option, which is a feature implemented by the GNU find binary. If the target does not support this option, such as HP-UX and AIX devices, users will need to enable 'thorough tests' in their scan policy to run the find command without using a '-maxdepth' argument.

See Also

https://openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/11/21, Modified: 2025/07/14

Plugin Output

tcp/0

```
Nessus detected 4 installs of OpenSSL:

  Path               : /opt/nessus/bin/openssl
  Version            : 3.0.16
  Associated Package : Nessus-10.9.1-el9.x86_64

  Path               : /opt/nessus/lib/nessus/libcrypto.so.3
  Version            : 3.0.16
  Associated Package : Nessus-10.9.1-el9.x86_64

  Path               : /usr/lib64/libcrypto.so.3.2.2
```

```
  Version            : 3.2.2
  Associated Package : openssl-libs-3.2.2-1.amzn2023.0.1.x86_64

  Path               : /usr/bin/openssl
  Version            : 3.2.2
  Associated Package : openssl-3.2.2-1.amzn2023.0.1
  Managed by OS      : True

We are unable to retrieve version info from the following list of OpenSSL files. However, these
 installs may include their version within the filename or the filename of the Associated Package.

e.g. libssl.so.3 (OpenSSL 3.x), libssl.so.1.1 (OpenSSL 1.1.x)

/opt/nessus/lib/nessus/libssl.so.3
/usr/lib64/libssl.so.3.2.2
```

179139 - Package Manager Packages Report (nix)

Synopsis

Reports details about packages installed via package managers.

Description

Reports details about packages installed via package managers

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/08/01, Modified: 2025/05/07

Plugin Output

tcp/0

```
Successfully retrieved and stored package data.
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/22/ssh

```
Process ID   : 2170
Executable   : /usr/sbin/sshd
Command line : sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

udp/68

```
Process ID   : 1939
Executable   : /usr/lib/systemd/systemd-networkd
Command line : /usr/lib/systemd/systemd-networkd
```

25221 - Remote listeners enumeration (Linux / AIX)

Synopsis

Using the supplied credentials, it was possible to identify the process listening on the remote port.

Description

By logging into the remote host with the supplied credentials, Nessus was able to obtain the name of the process listening on the remote port.

Note that the method used by this plugin only works for hosts running Linux or AIX.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2024/07/05

Plugin Output

tcp/8834/www

```
Process ID   : 2760
Executable   : /opt/nessus/sbin/nessusd
Command line : nessusd -q
```

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: 2025/07/14

Plugin Output

tcp/0

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

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

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

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

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-ed25519

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
```

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

The server supports the following options for mac_algorithms_server_to_client :

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

The server supports the following options for kex_algorithms :

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

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

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

10881 - SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

  - 1.99
  - 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled

Synopsis

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

Description

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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

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

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

10267 - SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

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

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.7
SSH supported authentication : publickey,gssapi-keyex,gssapi-with-mic
```

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: 2025/06/16

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: ip-172-31-94-8.ec2.internal

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: 12 BE

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jul 17 13:42:04 2025 GMT
Not Valid After: Jul 16 13:42:04 2029 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B8 E0 67 59 59 DA 46 71 47 B2 3E DF 9C B8 E4 FF FD 16 49
```

```
             18 0E 1F E2 57 E9 66 F9 C7 F8 71 BA 3F 42 FE 83 EC 80 0C 41
             43 5B 10 06 54 0F 0D 9A E1 3B CE 9F BF 24 50 3E EC 00 23 86
             49 75 9C 43 96 EA D9 CB C4 90 CA 52 79 78 63 85 0D 65 52 A3
             17 92 46 98 D4 10 2F C4 0D 3D F2 AC 50 8E 07 DE 18 8F 6A A0
             12 55 6F 08 B5 B0 E8 10 A3 FF 41 56 9E 6F 48 EB 04 60 37 45
             5B BD D8 F7 41 A8 7D EA AE 09 D1 BA 9E CE 3F 7B 86 85 24 CF
             98 CB 8B 1B 4B 31 44 0D E2 FE E2 0D 6F D4 20 12 A0 DA 19 C4
             EA 56 FE 05 4D 5F D7 CE 12 1F A1 80 BA 48 B1 EB BF 3D 6C 03
             99 97 40 88 99 66 05 DD 7C FE 45 4D 5B A6 6F 7D 79 30 17 40
             80 1A 08 9A 4A 6E D3 49 66 3B 78 54 88 67 4C D8 C0 7D 23 4A
             48 F6 DF 66 35 D1 1E 9E 82 C9 8F A6 13 CB 23 FF 61 7E 93 CC
             A2 5C 90 B8 57 03 DB 59 46 DF E5 03 38 EF 0E 55 F5
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 02 15 F0 0C 05 9A A7 25 F0 45 F2 FE 36 3C 27 B6 06 41 06
           33 15 82 D3 5D 4D 61 4C 84 5B 33 04 28 A0 50 93 3D F3 4C 27
           8C 34 9D A6 C8 D6 29 6F FB D5 DE E8 1A C8 4A 96 CC 76 D6 60
           87 FB 81 7D 87 D3 C9 8E DC 42 C8 3A 0C A6 15 00 FC 27 94 37
           1E EB 4D D2 63 7C 9F 48 21 1B 77 74 8B 3D 93 3C C7 86 B9 04
           26 39 D5 B0 16 FB 23 C8 92 1B 46 F3 BE 8A 26 02 FE E2 23 CF
          [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/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: 2024/03/26

Plugin Output

tcp/8834/www

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

tcp/8834/www

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

11153 - Service Detection (HELP Request)

Synopsis

The remote service could be identified.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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: 2025/03/26

Plugin Output

tcp/0

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

  device-mapper-libs-1.02.185-1.amzn2023.0.5|(none) Tue Jul  8 17:19:55 2025|Amazon Linux|Amazon
 Linux
  vim-data-9.1.1484-1.amzn2023.0.1|2 Tue Jul  8 17:19:49 2025|Amazon Linux|Amazon Linux
  kbd-2.4.0-2.amzn2023.0.3|(none) Tue Jul  8 17:19:55 2025|Amazon Linux|Amazon Linux
  python3-setuptools-wheel-59.6.0-2.amzn2023.0.6|(none) Tue Jul  8 17:19:49 2025|Amazon Linux|Amazon
 Linux
  libmount-2.37.4-1.amzn2023.0.4|(none) Tue Jul  8 17:19:55 2025|Amazon Linux|Amazon Linux
  pcre2-syntax-10.40-1.amzn2023.0.3|(none) Tue Jul  8 17:19:49 2025|Amazon Linux|Amazon Linux
  libblkid-2.37.4-1.amzn2023.0.4|(none) Tue Jul  8 17:19:55 2025|Amazon Linux|Amazon Linux
  kernel-livepatch-repo-s3-2023.8.20250707-0.amzn2023|(none) Tue Jul  8 17:19:49 2025|Amazon Linux|
Amazon Linux
  rpm-libs-4.16.1.3-29.amzn2023.0.6|(none) Tue Jul  8 17:19:56 2025|Amazon Linux|Amazon Linux
  system-release-2023.8.20250707-0.amzn2023|(none) Tue Jul  8 17:19:49 2025|Amazon Linux|Amazon
 Linux
  systemd-networkd-252.23-4.amzn2023|(none) Tue Jul  8 17:19:56 2025|Amazon Linux|Amazon Linux
  glibc-all-langpacks-2.34-196.amzn2023.0.1|(none) Tue Jul  8 17:19:51 2025|Amazon Linux|Amazon
 Linux
  dracut-102-3.amzn2023.0.1|(none) Tue Jul  8 17:19:57 2025|Amazon Linux|Amazon Linux
  zlib-1.2.11-33.amzn2023.0.5|(none) Tue Jul  8 17:19:51 2025|Amazon Linux|Amazon Linux
  grub2-tools-2.06-61.amzn2023.0.18|1 Tue Jul  8 17:19:57 2025|Amazon Linux|Amazon Linux
```

```
libstdc++-14.2.1-7.amzn2023.0.1|(none) Tue Jul  8 17:19:51 2025|Amazon Linux|Amazon Linux
libtirpc-1.3.3-0.amzn2023|(none) Tue Jul  8 17:19:58 2025|Amazon Linux|Amazon Linux
libcom_err-1.46.5-2.amzn2023.0.2|(none) Tue Jul  8 17:19:51 2025|Amazon Linux|Amazon Linux
openssh-8.7p1-8.amzn2023.0.15|(none) Tue Jul  8 17:20:16 2025|Amazon Linux|Amazon Linux
libxml2-2.10.4-1.amzn2023.0.11|(none) Tue Jul  8 17:19:51 2025|Amazon Linux|Amazon Linux
libmodulemd-2.13.0-2.amzn2023.0.2|(none) Tue Jul  8 17:20:16 2025|Amazon Linux|Amazon Linux [...]
```

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; includeSubDomains
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

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

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8834/www

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

110095 - Target Credential Issues by Authentication Protocol - No Issues Found

Synopsis

Nessus was able to log in to the remote host using the provided credentials. No issues were reported with access, privilege, or intermittent failure.

Description

Valid credentials were provided for an authentication protocol on the remote target and Nessus did not log any subsequent errors or failures for the authentication protocol.

When possible, Nessus tracks errors or failures related to otherwise valid credentials in order to highlight issues that may result in incomplete scan results or limited scan coverage. The types of issues that are tracked include errors that indicate that the account used for scanning did not have sufficient permissions for a particular check, intermittent protocol failures which are unexpected after the protocol has been negotiated successfully earlier in the scan, and intermittent authentication failures which are unexpected after a credential set has been accepted as valid earlier in the scan. This plugin reports when none of the above issues have been logged during the course of the scan for at least one authenticated protocol. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for issues to be encountered for one protocol and not another.

For example, authentication to the SSH service on the remote target may have consistently succeeded with no privilege errors encountered, while connections to the SMB service on the remote target may have failed intermittently.

- Resolving logged issues for all available authentication protocols may improve scan coverage, but the value of resolving each issue for a particular protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol and what particular check failed. For example, consistently successful checks via SSH are more critical for Linux targets than for Windows targets, and likewise consistently successful checks via SMB are more critical for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0520

Plugin Information

Published: 2018/05/24, Modified: 2024/03/25

Plugin Output

tcp/0

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

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

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

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

Please note the following :

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

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```
Nessus was able to execute commands on localhost.
```

163326 - Tenable Nessus Installed (Linux)

Synopsis

Tenable Nessus is installed on the remote Linux host.

Description

Tenable Nessus is installed on the remote Linux host.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2022/07/21, Modified: 2025/07/14

Plugin Output

tcp/0

```
Path    : /opt/nessus
Version : 10.9.1
Build   : 20006
```

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  6.1.141-165.249. Thu Jul 17 13:37   still running

wtmp begins Thu Jul 17 13:37:55 2025
```

192709 - Tukaani XZ Utils Installed (Linux / Unix)

Synopsis

Tukaani XZ Utils is installed on the remote Linux / Unix host.

Description

Tukaani XZ Utils is installed on the remote Linux / Unix host.

XZ Utils consists of several components, including:

- liblzma

- xz

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.192709' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://xz.tukaani.org/xz-utils/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/03/29, Modified: 2025/07/14

Plugin Output

tcp/0

```
Nessus detected 2 installs of XZ Utils:

  Path               : /usr/bin/xz
  Version            : 5.2.5
  Associated Package : xz-5.2.5-9.amzn2023.0.2.x86_64
  Confidence         : High
```

```
    Version Source     : Package

    Path               : /usr/lib64/liblzma.so.5.2.5
    Version            : 5.2.5
    Associated Package : xz-libs-5.2.5-9.amzn2023.0.2.x86_64
    Confidence         : High
    Version Source     : Package
```

110483 - Unix / Linux Running Processes Information

Synopsis

Uses /bin/ps auxww command to obtain the list of running processes on the target machine at scan time.

Description

Generated report details the running processes on the target machine at scan time.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/06/12, Modified: 2023/11/27

Plugin Output

tcp/0

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  1.1 107116 11648 ?        Ss   13:37   0:01 /usr/lib/systemd/systemd --
switched-root --system --deserialize=32
root           2  0.0  0.0      0     0 ?        S    13:37   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   13:37   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   13:37   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   13:37   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   13:37   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   13:37   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   13:37   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    13:37   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    13:37   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    13:37   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    13:37   0:00 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    13:37   0:00 [rcu_preempt]
root          16  0.0  0.0      0     0 ?        S    13:37   0:00 [migration/0]
root          18  0.0  0.0      0     0 ?        S    13:37   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    13:37   0:00 [kdevtmpfs]
root          21  0.0  0.0      0     0 ?        I<   13:37   0:00 [inet_frag_wq]
root          22  0.0  0.0      0     0 ?        S    13:37   0:00 [kauditd]
root          23  0.0  0.0      0     0 ?        S    13:37   0:00 [khungtaskd]
root          24  0.0  0.0      0     0 ?        S    13:37   0:00 [oom_reaper]
root          27  0.0  0.0      0     0 ?        I<   13:37   0:00 [writeback]
root          28  0.0  0.0      0     0 ?        S    13:37   0:01 [kcompactd0]
root          29  0.0  0.0      0     0 ?        SN   13:37   0:00 [khugepaged]
root          30  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
```

189731 - Vim Installed (Linux)

Synopsis

Vim is installed on the remote Linux host.

Description

Vim is installed on the remote Linux host.

See Also

https://www.vim.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2024/01/29, Modified: 2025/07/14

Plugin Output

tcp/0

```
Path    : /usr/bin/vim
Version : 9.1
```

138014 - kpatch : Installed Patches

Synopsis

The remote host is using kpatch to maintain the OS kernel.

Description

kpatch is being used to maintain the remote host's operating system kernel without requiring reboots.

See Also

https://github.com/dynup/kpatch

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/07/01, Modified: 2021/05/10

Plugin Output

tcp/0

```
kpatch is installed, but no loaded patch modules appear to cover any CVEs.
kpatch list output:

Loaded patch modules:

Installed patch modules:
```

182848 - libcurl Installed (Linux / Unix)

Synopsis

libcurl is installed on the remote Linux / Unix host.

Description

libcurl is installed on the remote Linux / Unix host.

Additional information:

- More paths will be searched and the timeout for the search will be increased if 'Perform thorough tests' setting is enabled.

- The plugin timeout can be set to a custom value other than the plugin's default of 30 minutes via the 'timeout.182848' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

See Also

https://curl.se/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/10/10, Modified: 2025/07/14

Plugin Output

tcp/0

```
Path               : /usr/lib64/libcurl.so.4.8.0
Version            : 8.11.1
Associated Package : libcurl-minimal-8.11.1-4.amzn2023.0.1.x86_64
```