# Advanced Scan

Report generated by Tenable Nessus™ Mon, 12 Aug 2024 14:14:58 CEST

## Vulnerabilities by Host

# Vulnerabilities by Host

# 192.168.110.1

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 181 | 125 | 217 | 0 | 108 |

## Scan Information

Start time: Mon Aug 12 13:48:32 2024

End time: Mon Aug 12 14:08:37 2024

## Host Information

IP: 192.168.110.1

MAC Address: 3C:EC:EF:DE:9D:5E 3C:EC:EF:DE:9A:C5 3C:EC:EF:DD:55:E1 3C:EC:EF:DE:9A:C4 3C:EC:EF:DE:9A:C2 3C:EC:EF:DE:9D:5F 3C:EC:EF:DD:55:E0 3C:EC:EF:DD:55:DE 3C:EC:EF:DE:9B:CE 02:42:1E:55:59:53 3C:EC:EF:DE:9B:CF 3C:EC:EF:DD:55:DF B0:3A:F2:B6:05:9F

OS: Linux Kernel 5.15.0-87-generic on Ubuntu 22.04

## Vulnerabilities

### 204784 - Docker Engine < 23.0.15 / 26.x < 26.1.5 / 27.x < 27.1.1 Authentication Bypass

#### Synopsis

The remote host has an application installed that is affected by an authentication bypass vulnerability.

#### Description

The version of the Docker Engine (Moby) installed on the remote host is prior to 23.0.15, 26.x prior to 26.1.5 or 27.x prior to 27.1.1. It is therefore affected by an authentication bypass vulnerability. Using a specially-crafted API request, an Engine API client could make the daemon forward the request or response to an authorization plugin without the body. In certain circumstances, the authorization plugin may allow a request which it would have otherwise denied if the body had been forwarded to it. A security issue was discovered In 2018, where an attacker could bypass AuthZ plugins using a specially crafted API request. This could lead to unauthorized actions, including privilege escalation. Although this issue was fixed in Docker Engine v18.09.1 in January 2019, the fix was not carried forward to later major versions, resulting in a regression. Anyone who depends on authorization plugins that introspect the request and/or response body to make access control decisions is potentially impacted.

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

#### See Also

https://github.com/moby/moby/security/advisories/GHSA-v23v-6jw2-98fq
http://www.nessus.org/u?d718ad8d

## Solution

Upgrade to Docker Engine version 23.0.15, 26.1.5, 27.1.1 or later

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

10.0

## EPSS Score

0.0004

## CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-41110 |
| XREF | IAVA:2024-A-0438 |

## Plugin Information

Published: 2024/07/26, Modified: 2024/07/29

## Plugin Output

### tcp/0

```
Path              : /usr/bin/docker
Installed version : 26.1.4
Fixed version     : Upgrade to 23.0.15, 26.1.5, 27.1.1 or later.
```

## 152782 - OpenSSL 1.1.1 < 1.1.1l Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1l. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1l advisory.

- ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the data and length fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the data field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack).

It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y). (CVE-2021-3712)

- In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the out parameter can be NULL and, on exit, the outlen parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the out parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

(CVE-2021-3711)

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

## See Also

http://www.nessus.org/u?4e69aead
http://www.nessus.org/u?77bbd34b
https://www.cve.org/CVERecord?id=CVE-2021-3711
https://www.cve.org/CVERecord?id=CVE-2021-3712
https://www.openssl.org/news/secadv/20210824.txt

## Solution

Upgrade to OpenSSL version 1.1.1l or later.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## EPSS Score

0.0679

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2021-3711 |
| CVE | CVE-2021-3712 |

XREF IAVA:2021-A-0395-S

## Plugin Information

Published: 2021/08/24, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
```

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

## 160477 - OpenSSL 1.1.1 < 1.1.1o Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).

Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd). (CVE-2022-1292)

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

### See Also

http://www.nessus.org/u?4d87f2b7

https://www.cve.org/CVERecord?id=CVE-2022-1292

https://www.openssl.org/news/secadv/20220503.txt

### Solution

Upgrade to OpenSSL version 1.1.1o or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

EPSS Score

0.1283

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-1292 |
| XREF | IAVA:2022-A-0186-S |

Plugin Information

Published: 2022/05/03, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

## 162420 - OpenSSL 1.1.1 < 1.1.1p Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). (CVE-2022-2068)

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

### See Also

http://www.nessus.org/u?33d5d7fb

https://www.cve.org/CVERecord?id=CVE-2022-2068

https://www.openssl.org/news/secadv/20220621.txt

### Solution

Upgrade to OpenSSL version 1.1.1p or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

EPSS Score

0.0932

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2022-2068 |

Plugin Information

Published: 2022/06/21, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
    Fixed version    : 1.1.1p
```

tcp/0

```
    Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
    Reported version : 1.1.1k
    Fixed version    : 1.1.1p
```

## 201084 - OpenSSL 1.1.1 < 1.1.1za Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 1.1.1za (premium support) (Affected since 1.1.1). (CVE-2024-5535)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 1.1.1za or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-5535 |

Plugin Information

Published: 2024/06/27, Modified: 2024/07/03

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9768992a25e6f6e963c9a3b5c4af5981944da49558318bb00e91f523ddfdd2df/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

## 201085 - OpenSSL 3.0.0 < 3.0.15 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.15. It is, therefore, affected by a vulnerability as referenced in the 3.0.15 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 1.1.1za (premium support) (Affected since 1.1.1). (CVE-2024-5535)

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

See Also

http://www.nessus.org/u?8f2a60eb

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 3.0.15 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-5535 |

Plugin Information

Published: 2024/06/27, Modified: 2024/07/03

Plugin Output

tcp/0

```
  Path             : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.15
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.15
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.15
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.15
```

## 160473 - OpenSSL 3.0.0 < 3.0.3 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.3. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.3 advisory.

- The OPENSSL_LH_flush() function, which empties a hash table, contains a bug that breaks reuse of the memory occuppied by the removed hash table entries. This function is used when decoding certificates or keys. If a long lived process periodically decodes certificates or keys its memory usage will expand without bounds and the process might be terminated by the operating system causing a denial of service.

Also traversing the empty hash table entries will take increasingly more time. Typically such long lived processes might be TLS clients or TLS servers configured to accept client certificate authentication. The function was added in the OpenSSL 3.0 version thus older releases are not affected by the issue. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). (CVE-2022-1473)

- The OpenSSL 3.0 implementation of the RC4-MD5 ciphersuite incorrectly uses the AAD data as the MAC key.

This makes the MAC key trivially predictable. An attacker could exploit this issue by performing a man-in-the-middle attack to modify data being sent from one endpoint to an OpenSSL 3.0 recipient such that the modified data would still pass the MAC integrity check. Note that data sent from an OpenSSL 3.0 endpoint to a non-OpenSSL 3.0 endpoint will always be rejected by the recipient and the connection will fail at that point. Many application protocols require data to be sent from the client to the server first.

Therefore, in such a case, only an OpenSSL 3.0 server would be impacted when talking to a non-OpenSSL 3.0 client. If both endpoints are OpenSSL 3.0 then the attacker could modify data being sent in both directions. In this case both clients and servers could be affected, regardless of the application protocol. Note that in the absence of an attacker this bug means that an OpenSSL 3.0 endpoint communicating with a non-OpenSSL 3.0 endpoint will fail to complete the handshake when using this ciphersuite. The confidentiality of data is not impacted by this issue, i.e. an attacker cannot decrypt data that has been encrypted using this ciphersuite - they can only modify it. In order for this attack to work both endpoints must legitimately negotiate the RC4-MD5 ciphersuite. This ciphersuite is not compiled by default in OpenSSL 3.0, and is not available within the default provider or the default ciphersuite list. This ciphersuite will never be used if TLSv1.3 has been negotiated. In order for an OpenSSL 3.0 endpoint to use this ciphersuite the following must have occurred: 1) OpenSSL must have been compiled with the (non-default) compile time option enable-weak-ssl-ciphers 2) OpenSSL must have had the legacy provider explicitly loaded (either through application code or via configuration) 3) The ciphersuite must have been explicitly added to the ciphersuite list 4) The libssl security level must have been set to 0 (default is 1) 5) A version of SSL/TLS below TLSv1.3 must have been negotiated 6) Both endpoints must negotiate the RC4-MD5 ciphersuite in preference to any others that both endpoints have in common Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). (CVE-2022-1434)

- The function `OCSP_basic_verify` verifies the signer certificate on an OCSP response. In the case where the (non-default) flag OCSP_NOCHECKS is used then the response will be positive (meaning a successful verification) even in the case where the response signing certificate fails to verify. It is anticipated that most users of `OCSP_basic_verify` will not use the OCSP_NOCHECKS flag. In this case the `OCSP_basic_verify` function will return a negative value (indicating a fatal error) in the case of a certificate verification failure. The normal expected return value in this case would be 0. This issue also impacts the command line OpenSSL ocsp application. When verifying an ocsp response with the

-no_cert_checks option the command line application will report that the verification is successful even though it has in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). (CVE-2022-1343)

- The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).

Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd). (CVE-2022-1292)

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://www.cve.org/CVERecord?id=CVE-2022-1292

https://www.cve.org/CVERecord?id=CVE-2022-1343

https://www.cve.org/CVERecord?id=CVE-2022-1434

https://www.cve.org/CVERecord?id=CVE-2022-1473

http://www.nessus.org/u?a704d771

http://www.nessus.org/u?ea9b1d96

https://www.openssl.org/news/secadv/20220503.txt

http://www.nessus.org/u?4e726fd8

http://www.nessus.org/u?7cec6b9a

## Solution

Upgrade to OpenSSL version 3.0.3 or later.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

EPSS Score

0.1283

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-1292 |
| CVE | CVE-2022-1343 |
| CVE | CVE-2022-1434 |
| CVE | CVE-2022-1473 |
| XREF | IAVA:2022-A-0186-S |

Plugin Information

Published: 2022/05/03, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.3
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.3
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.3
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.3
```

## 162418 - OpenSSL 3.0.0 < 3.0.4 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.4. It is, therefore, affected by a vulnerability as referenced in the 3.0.4 advisory.

- In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). (CVE-2022-2068)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-2068

http://www.nessus.org/u?8c2076d9

https://www.openssl.org/news/secadv/20220621.txt

### Solution

Upgrade to OpenSSL version 3.0.4 or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

EPSS Score

0.0932

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-2068 |
| XREF | IAVA:2022-A-0257-S |

Plugin Information

Published: 2022/06/21, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.4
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.4
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.4
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.4
```

## 162720 - OpenSSL 3.0.0 < 3.0.5 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.5. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.5 advisory.

- The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such machines and memory corruption will happen during the computation. As a consequence of the memory corruption an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048 bit RSA private keys running on machines supporting AVX512IFMA instructions of the X86_64 architecture are affected by this issue. (CVE-2022-2274)

- AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of in place encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). (CVE-2022-2097)

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

### See Also

http://www.nessus.org/u?05ef5c2c

http://www.nessus.org/u?58b324e2

https://www.openssl.org/news/secadv/20220705.txt

https://www.cve.org/CVERecord?id=CVE-2022-2097

https://www.cve.org/CVERecord?id=CVE-2022-2274

### Solution

Upgrade to OpenSSL version 3.0.5 or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0224

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-2097 |
| CVE | CVE-2022-2274 |
| XREF | IAVA:2022-A-0265-S |

Plugin Information

Published: 2022/07/05, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.5
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
```

```
  Fixed version    : 3.0.5
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.5
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.5
```

## 201082 - OpenSSL 3.1.0 < 3.1.7 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.7. It is, therefore, affected by a vulnerability as referenced in the 3.1.7 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 3.3.2 (Affected since 3.3.0). (CVE-2024-5535)

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

See Also

http://www.nessus.org/u?f87142a6

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 3.1.7 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-5535 |

Plugin Information

Published: 2024/06/27, Modified: 2024/07/03

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/2bbb5ec3fdcf5666e9849822366e5d09a7a4c0aa114e6f17d554f73ea9356d1c/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.7
```

## 182308 - OpenSSL SEoL (1.1.1.x)

### Synopsis

An unsupported version of OpenSSL is installed on the remote host.

### Description

According to its version, OpenSSL is 1.1.1.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

### See Also

https://www.openssl.org/blog/blog/2023/09/11/eol-111/

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

https://www.openssl.org/news/vulnerabilities-1.1.1.html

### Solution

Upgrade to a version of OpenSSL that is currently supported.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2023/09/29, Modified: 2024/05/31

### Plugin Output

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
```

```
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                     : 1.1.1k
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                     : 1.1.1k
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Installed version                     : 1.1.1k
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Installed version                     : 1.1.1k
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Installed version                     : 1.1.1k
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/bin/openssl
```

```
  Installed version                     : 1.1.1w
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                     : 1.1.1w
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                     : 1.1.1w
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Installed version                     : 1.1.1n
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Installed version                     : 1.1.1n
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Installed version                     : 1.1.1k
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Installed version                       : 1.1.1n
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Installed version                       : 1.1.1w
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Installed version                       : 1.1.1w
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/9768992a25e6f6e963c9a3b5c4af5981944da49558318bb00e91f523ddfdd2df/diff/usr/bin/openssl
  Installed version                       : 1.1.1w
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
```

```
   Time since Security End of Life (Est.) : >= 6 months
```

## 202187 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Python vulnerabilities (USN-6891-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6891-1 advisory.

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.

(CVE-2015-20107)

It was discovered that Python incorrectly used regular expressions vulnerable to catastrophic backtracking. A remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2018-1060, CVE-2018-1061)

It was discovered that Python failed to initialize Expats hash salt. A remote attacker could possibly use this issue to cause hash collisions, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2018-14647)

It was discovered that Python incorrectly handled certain pickle files. An attacker could possibly use this issue to consume memory, leading to a denial of service. This issue only affected Ubuntu 14.04 LTS.

(CVE-2018-20406)

It was discovered that Python incorrectly validated the domain when handling cookies. An attacker could possibly trick Python into sending cookies to the wrong domain. This issue only affected Ubuntu 14.04 LTS.

(CVE-2018-20852)

Jonathan Birch and Panayiotis Panayiotou discovered that Python incorrectly handled Unicode encoding during NFKC normalization. An attacker could possibly use this issue to obtain sensitive information. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-9636, CVE-2019-10160)

It was discovered that Python incorrectly parsed certain email addresses. A remote attacker could possibly use this issue to trick Python applications into accepting email addresses that should be denied. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-16056)

It was discovered that the Python documentation XML-RPC server incorrectly handled certain fields. A remote attacker could use this issue to execute a cross-site scripting (XSS) attack. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-16935)

It was discovered that Python documentation had a misleading information. A security issue could be possibly caused by wrong assumptions of this information. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-17514)

It was discovered that Python incorrectly stripped certain characters from requests. A remote attacker could use this issue to perform CRLF injection. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2019-18348)

It was discovered that Python incorrectly handled certain TAR archives. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.

(CVE-2019-20907)

Colin Read and Nicolas Edet discovered that Python incorrectly handled parsing certain X509 certificates.

An attacker could possibly use this issue to cause Python to crash, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-5010)

It was discovered that incorrectly handled certain ZIP files. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-9674)

It was discovered that Python incorrectly handled certain urls. A remote attacker could possibly use this issue to perform CRLF injection attacks. This issue only affected Ubuntu 14.04 LTS. (CVE-2019-9740, CVE-2019-9947)

Sihoon Lee discovered that Python incorrectly handled the local_file: scheme. A remote attacker could possibly use this issue to bypass blocklist meschanisms. This issue only affected Ubuntu 14.04 LTS.

(CVE-2019-9948)

It was discovered that Python incorrectly handled certain IP values. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.

(CVE-2020-14422)

It was discovered that Python incorrectly handled certain character sequences. A remote attacker could possibly use this issue to perform CRLF injection. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2020-26116)

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code or cause a denial of service. This issue only affected Ubuntu 14.04 LTS.

(CVE-2020-27619, CVE-2021-3177)

It was discovered that Python incorrectly handled certain HTTP requests. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2020-8492)

It was discovered that the Python stdlib ipaddress API incorrectly handled octal strings. A remote attacker could possibly use this issue to perform a wide variety of attacks, including bypassing certain access restrictions. This issue only affected Ubuntu 18.04 LTS. (CVE-2021-29921)

David Schwrer discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. (CVE-2021-3426)

It was discovered that Python incorrectly handled certain RFCs. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2021-3733)

It was discovered that Python incorrectly handled certain server responses. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS. (CVE-2021-3737)

It was discovered that Python incorrectly handled certain FTP requests. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2021-4189)

It was discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS.

(CVE-2022-0391)

Devin Jeanpierre discovered that Python incorrectly handled sockets when the multiprocessing module was being used. A local attacker could possibly use this issue to execute arbitrary code and escalate privileges. This issue only affected Ubuntu 22.04 LTS. (CVE-2022-42919)

It was discovered that Python incorrectly handled certain inputs. If a user or an automated system were tricked into running a specially crafted input, a remote attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS and Ubuntu 22.04 LTS.

(CVE-2022-45061, CVE-2023-24329)

It was discovered that Python incorrectly handled certain scripts. An attacker could possibly use this issue to execute arbitrary code or cause a crash. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48560)

It was discovered that Python incorrectly handled certain plist files. If a user or an automated system were tricked into processing a specially crafted plist file, an attacker could possibly use this issue to consume resources, resulting in a denial of service. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48564)

It was discovered that Python did not properly handle XML entity declarations in plist files. An attacker could possibly use this vulnerability to perform an XML External Entity (XXE) injection, resulting in a denial of service or information disclosure. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48565)

It was discovered that Python did not properly provide constant-time processing for a crypto operation. An attacker could possibly use this issue to perform a timing attack and recover sensitive information. This issue only affected Ubuntu 14.04 LTS and Ubuntu 18.04 LTS. (CVE-2022-48566)

It was discovered that Python instances of ssl.SSLSocket were vulnerable to a bypass of the TLS handshake.

An attacker could possibly use this issue to cause applications to treat unauthenticated received data before TLS handshake as authenticated data after TLS handshake. This issue only affected Ubuntu 14.04 LTS, Ubuntu 18.04 LTS, Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. (CVE-2023-40217)

It was discovered that Python incorrectly handled null bytes when normalizing pathnames. An attacker could possibly use this issue to bypass certain filename checks. This issue only affected Ubuntu 22.04 LTS.

(CVE-2023-41105)

It was discovered that Python incorrectly handled privilege with certain parameters. An attacker could possibly use this issue to maintain the original processes' groups before starting the new process. This issue only affected Ubuntu 23.10. (CVE-2023-6507)

It was discovered that Python incorrectly handled symlinks in temp files. An attacker could possibly use this issue to modify the permissions of files. This issue only affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 23.10. (CVE-2023-6597)

It was discovered that Python incorrectly handled certain crafted zip files. An attacker could possibly use this issue to crash the program, resulting in a denial of service. (CVE-2024-0450)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6891-1

## Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0384

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2015-20107 |
| CVE | CVE-2018-1060 |
| CVE | CVE-2018-1061 |
| CVE | CVE-2018-14647 |
| CVE | CVE-2018-20406 |
| CVE | CVE-2018-20852 |
| CVE | CVE-2019-5010 |
| CVE | CVE-2019-9636 |
| CVE | CVE-2019-9674 |
| CVE | CVE-2019-9740 |
| CVE | CVE-2019-9947 |
| CVE | CVE-2019-9948 |
| CVE | CVE-2019-10160 |
| CVE | CVE-2019-16056 |
| CVE | CVE-2019-16935 |
| CVE | CVE-2019-17514 |
| CVE | CVE-2019-18348 |

| | |
|---|---|
| CVE | CVE-2019-20907 |
| CVE | CVE-2020-8492 |
| CVE | CVE-2020-14422 |
| CVE | CVE-2020-26116 |
| CVE | CVE-2020-27619 |
| CVE | CVE-2021-3177 |
| CVE | CVE-2021-3426 |
| CVE | CVE-2021-3733 |
| CVE | CVE-2021-3737 |
| CVE | CVE-2021-4189 |
| CVE | CVE-2021-29921 |
| CVE | CVE-2022-0391 |
| CVE | CVE-2022-42919 |
| CVE | CVE-2022-45061 |
| CVE | CVE-2022-48560 |
| CVE | CVE-2022-48564 |
| CVE | CVE-2022-48565 |
| CVE | CVE-2022-48566 |
| CVE | CVE-2023-6507 |
| CVE | CVE-2023-6597 |
| CVE | CVE-2023-24329 |
| CVE | CVE-2023-40217 |
| CVE | CVE-2023-41105 |
| CVE | CVE-2024-0450 |
| XREF | USN:6891-1 |

## Plugin Information

Published: 2024/07/11, Modified: 2024/07/11

## Plugin Output

tcp/0

```
  - Installed package : libpython3.10_3.10.12-1~22.04.3
  - Fixed package     : libpython3.10_3.10.12-1~22.04.4

  - Installed package : libpython3.10-minimal_3.10.12-1~22.04.3
  - Fixed package     : libpython3.10-minimal_3.10.12-1~22.04.4

  - Installed package : libpython3.10-stdlib_3.10.12-1~22.04.3
  - Fixed package     : libpython3.10-stdlib_3.10.12-1~22.04.4

  - Installed package : python3.10_3.10.12-1~22.04.3
  - Fixed package     : python3.10_3.10.12-1~22.04.4

  - Installed package : python3.10-minimal_3.10.12-1~22.04.3
  - Fixed package     : python3.10-minimal_3.10.12-1~22.04.4
```

## 204924 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenSSL vulnerabilities (USN-6937-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6937-1 advisory.

It was discovered that OpenSSL incorrectly handled TLSv1.3 sessions when certain non-default TLS server configurations were in use. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. (CVE-2024-2511)

It was discovered that OpenSSL incorrectly handled checking excessively long DSA keys or parameters. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-4603)

William Ahern discovered that OpenSSL incorrectly handled certain memory operations in a rarely-used API.

A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-4741)

Joseph Birr-Pixton discovered that OpenSSL incorrectly handled calling a certain API with an empty supported client protocols buffer. A remote attacker could possibly use this issue to obtain sensitive information, or cause OpenSSL to crash, resulting in a denial of service. (CVE-2024-5535)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6937-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4603 |
| CVE | CVE-2024-4741 |
| CVE | CVE-2024-5535 |
| XREF | IAVA:2024-A-0208-S |
| XREF | IAVA:2024-A-0321 |
| XREF | USN:6937-1 |

Plugin Information

Published: 2024/07/31, Modified: 2024/07/31

Plugin Output

tcp/0

```
  - Installed package : libssl3_3.0.2-0ubuntu1.16
  - Fixed package     : libssl3_3.0.2-0ubuntu1.17

  - Installed package : openssl_3.0.2-0ubuntu1.16
  - Fixed package     : openssl_3.0.2-0ubuntu1.17
```

## 186078 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6496-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6496-1 advisory.

- Improper access control in the Intel(R) Ethernet Controller RDMA driver for linux before version 1.9.30 may allow an unauthenticated user to potentially enable escalation of privilege via network access.

(CVE-2023-25775)

- An issue was discovered in drivers/mtd/ubi/cdev.c in the Linux kernel 6.2. There is a divide-by-zero error in do_div(sz,mtd->erasesize), used indirectly by ctrl_cdev_ioctl, when mtd->erasesize is 0.

(CVE-2023-31085)

- An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.5.3. A buffer size may not be adequate for frames larger than the MTU. (CVE-2023-45871)

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://ubuntu.com/security/notices/USN-6496-1

### Solution

Update the affected kernel package.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

## EPSS Score

0.0008

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-25775 |
| CVE | CVE-2023-31085 |
| CVE | CVE-2023-45871 |
| XREF | USN:6496-1 |

## Plugin Information

Published: 2023/11/21, Modified: 2024/01/09

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-89-generic
 for this advisory.
```

## 193084 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6725-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6725-1 advisory.

Chih-Yen Chang discovered that the KSMBD implementation in the Linux kernel did not properly validate certain data structure fields when parsing lease contexts, leading to an out-of-bounds read vulnerability.

A remote attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-1194)

Quentin Minster discovered that a race condition existed in the KSMBD implementation in the Linux kernel, leading to a use-after-free vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-32254)

It was discovered that a race condition existed in the KSMBD implementation in the Linux kernel when handling session connections, leading to a use- after-free vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2023-32258)

It was discovered that the KSMBD implementation in the Linux kernel did not properly validate buffer sizes in certain operations, leading to an integer underflow and out-of-bounds read vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-38427)

Chih-Yen Chang discovered that the KSMBD implementation in the Linux kernel did not properly validate SMB request protocol IDs, leading to a out-of- bounds read vulnerability. A remote attacker could possibly use this to cause a denial of service (system crash). (CVE-2023-38430)

Chih-Yen Chang discovered that the KSMBD implementation in the Linux kernel did not properly validate packet header sizes in certain situations, leading to an out-of-bounds read vulnerability. A remote attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2023-38431)

It was discovered that the KSMBD implementation in the Linux kernel did not properly handle session setup requests, leading to an out-of-bounds read vulnerability. A remote attacker could use this to expose sensitive information. (CVE-2023-3867)

Pratyush Yadav discovered that the Xen network backend implementation in the Linux kernel did not properly handle zero length data request, leading to a null pointer dereference vulnerability. An attacker in a guest VM could possibly use this to cause a denial of service (host domain crash). (CVE-2023-46838)

It was discovered that the IPv6 implementation of the Linux kernel did not properly manage route cache memory usage. A remote attacker could use this to cause a denial of service (memory exhaustion).

(CVE-2023-52340)

It was discovered that the device mapper driver in the Linux kernel did not properly validate target size during certain memory allocations. A local attacker could use this to cause a denial of service (system crash). (CVE-2023-52429, CVE-2024-23851)

Yang Chaoming discovered that the KSMBD implementation in the Linux kernel did not properly validate request buffer sizes, leading to an out-of-bounds read vulnerability. An attacker could use this to cause a denial of service (system crash) or possibly expose sensitive information. (CVE-2024-22705)

Chenyuan Yang discovered that the btrfs file system in the Linux kernel did not properly handle read operations on newly created subvolumes in certain conditions. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-23850)

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel, leading to a null pointer dereference vulnerability. A privileged local attacker could use this to possibly cause a denial of service (system crash). (CVE-2024-24860)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- Architecture specifics;

- Block layer;

- Cryptographic API;

- Android drivers;

- EDAC drivers;

- GPU drivers;

- Media drivers;

- Multifunction device drivers;

- MTD block device drivers;

- Network drivers;

- NVME drivers;

- TTY drivers;

- Userspace I/O drivers;

- EFI Variable file system;

- F2FS file system;

- GFS2 file system;

- SMB network file system;

- BPF subsystem;

- IPv6 Networking;

- Network Traffic Control;

- AppArmor security module; (CVE-2023-52463, CVE-2023-52445, CVE-2023-52462, CVE-2023-52609, CVE-2023-52448, CVE-2023-52457, CVE-2023-52464, CVE-2023-52456, CVE-2023-52454, CVE-2023-52438, CVE-2023-52480, CVE-2023-52443, CVE-2023-52442, CVE-2024-26631, CVE-2023-52439, CVE-2023-52612, CVE-2024-26598, CVE-2024-26586, CVE-2024-26589, CVE-2023-52444, CVE-2023-52436, CVE-2024-26633,

CVE-2024-26597, CVE-2023-52458, CVE-2024-26591, CVE-2023-52449, CVE-2023-52467, CVE-2023-52441, CVE-2023-52610, CVE-2023-52451, CVE-2023-52469, CVE-2023-52470)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6725-1

## Solution

Update the affected kernel package.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

## EPSS Score

0.0032

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-1194 |
| CVE | CVE-2023-3867 |
| CVE | CVE-2023-32254 |

| | |
|---|---|
| CVE | CVE-2023-32258 |
| CVE | CVE-2023-38427 |
| CVE | CVE-2023-38430 |
| CVE | CVE-2023-38431 |
| CVE | CVE-2023-46838 |
| CVE | CVE-2023-52340 |
| CVE | CVE-2023-52429 |
| CVE | CVE-2023-52436 |
| CVE | CVE-2023-52438 |
| CVE | CVE-2023-52439 |
| CVE | CVE-2023-52441 |
| CVE | CVE-2023-52442 |
| CVE | CVE-2023-52443 |
| CVE | CVE-2023-52444 |
| CVE | CVE-2023-52445 |
| CVE | CVE-2023-52448 |
| CVE | CVE-2023-52449 |
| CVE | CVE-2023-52451 |
| CVE | CVE-2023-52454 |
| CVE | CVE-2023-52456 |
| CVE | CVE-2023-52457 |
| CVE | CVE-2023-52458 |
| CVE | CVE-2023-52462 |
| CVE | CVE-2023-52463 |
| CVE | CVE-2023-52464 |
| CVE | CVE-2023-52467 |
| CVE | CVE-2023-52469 |
| CVE | CVE-2023-52470 |
| CVE | CVE-2023-52480 |
| CVE | CVE-2023-52609 |
| CVE | CVE-2023-52610 |
| CVE | CVE-2023-52612 |
| CVE | CVE-2024-22705 |
| CVE | CVE-2024-23850 |
| CVE | CVE-2024-23851 |
| CVE | CVE-2024-24860 |
| CVE | CVE-2024-26586 |
| CVE | CVE-2024-26589 |
| CVE | CVE-2024-26591 |
| CVE | CVE-2024-26597 |
| CVE | CVE-2024-26598 |
| CVE | CVE-2024-26631 |
| CVE | CVE-2024-26633 |

XREF USN:6725-1

## Plugin Information

Published: 2024/04/09, Modified: 2024/05/28

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-102-
generic for this advisory.
```

## 158974 - OpenSSL 1.1.1 < 1.1.1n Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self- signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc). (CVE-2022-0778)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-0778

http://www.nessus.org/u?2a52134e

https://www.openssl.org/news/secadv/20220315.txt

### Solution

Upgrade to OpenSSL version 1.1.1n or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.0134

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-0778 |
| XREF | IAVA:2022-A-0121-S |

Plugin Information

Published: 2022/03/16, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
```

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
```

```
    Fixed version    : 1.1.1n
```

## 171079 - OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1t. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1t advisory.

- There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName.

X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network. (CVE-2023-0286)

- The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected. (CVE-2023-0215)

- The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the name (e.g.

CERTIFICATE), any header data and the payload data. If the function succeeds then the name_out, header and data arguments are populated with pointers to buffers containing the relevant decoded data.

The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the

PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue. (CVE-2022-4450)

- A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption.

The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection. (CVE-2022-4304)

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://www.cve.org/CVERecord?id=CVE-2023-0286

https://www.openssl.org/news/secadv/20230207.txt

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

https://www.cve.org/CVERecord?id=CVE-2023-0215

https://www.cve.org/CVERecord?id=CVE-2022-4450

https://www.cve.org/CVERecord?id=CVE-2022-4304

## Solution

Upgrade to OpenSSL version 1.1.1t or later.

## 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:N/A:H)

## CVSS v3.0 Temporal Score

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

## VPR Score

6.0

## EPSS Score

0.0049

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2022-4304 |
| CVE | CVE-2022-4450 |
| CVE | CVE-2023-0215 |
| CVE | CVE-2023-0286 |

### Plugin Information

Published: 2023/02/07, Modified: 2024/06/07

### Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

## 181288 - OpenSSL 1.1.1 < 1.1.1w Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroized so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000 The FIPS provider is not affected by this issue.

(CVE-2023-4807)

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

### See Also

http://www.nessus.org/u?05c4bf30

https://www.cve.org/CVERecord?id=CVE-2023-4807

https://www.openssl.org/news/secadv/20230908.txt

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

### Solution

Upgrade to OpenSSL version 1.1.1w or later.

### Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-4807 |
| XREF | IAVA:2023-A-0462-S |

Plugin Information

Published: 2023/09/12, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
```

```
  Reported version : 1.1.1n
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

## 181289 - OpenSSL 3.0.0 < 3.0.11 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.11. It is, therefore, affected by a vulnerability as referenced in the 3.0.11 advisory.

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroized so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000 The FIPS provider is not affected by this issue.

(CVE-2023-4807)

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

### See Also

http://www.nessus.org/u?eeb05f22

https://www.cve.org/CVERecord?id=CVE-2023-4807

https://www.openssl.org/news/secadv/20230908.txt

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

### Solution

Upgrade to OpenSSL version 3.0.11 or later.

### Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-4807 |
| XREF | IAVA:2023-A-0462-S |

Plugin Information

Published: 2023/09/12, Modified: 2024/06/07

Plugin Output

tcp/0

```
Path              : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
Reported version : 3.0.2
Fixed version     : 3.0.11
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.11
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.11
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.11
```

## 183891 - OpenSSL 3.0.0 < 3.0.12 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.12. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.12 advisory.

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

- Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths.

This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers.

Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the keylen parameter or the IV length, via the ivlen parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.

(CVE-2023-5363)

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

## See Also

http://www.nessus.org/u?608327d1

http://www.nessus.org/u?71a978e4

https://www.cve.org/CVERecord?id=CVE-2023-5363

https://www.cve.org/CVERecord?id=CVE-2023-6129

## Solution

Upgrade to OpenSSL version 3.0.12 or later.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

5.0

## EPSS Score

0.0016

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-5363 |
| CVE | CVE-2023-6129 |
| XREF | IAVA:2023-A-0582-S |

## Plugin Information

Published: 2023/10/25, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path              : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.12
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.12
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.12
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.12
```

## 166047 - OpenSSL 3.0.0 < 3.0.6 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.6. It is, therefore, affected by a vulnerability as referenced in the 3.0.6 advisory.

- OpenSSL supports creating a custom cipher via the legacy EVP_CIPHER_meth_new() function and associated function calls. This function was deprecated in OpenSSL 3.0 and application authors are instead encouraged to use the new provider mechanism in order to implement custom ciphers. OpenSSL versions 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() and EVP_CipherInit_ex2() functions (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom cipher directly it incorrectly tries to fetch an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to EVP_CIPHER_meth_new(). This NID is supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pass NID_undef as this value in the call to EVP_CIPHER_meth_new(). When NID_undef is used in this way the OpenSSL encryption/decryption initialisation function will match the NULL cipher as being equivalent and will fetch this from the available providers.

This will succeed if the default provider has been loaded (or if a third party provider has been loaded that offers this cipher). Using the NULL cipher means that the plaintext is emitted as the ciphertext.

Applications are only affected by this issue if they call EVP_CIPHER_meth_new() using NID_undef and subsequently use it in a call to an encryption/decryption initialisation function. Applications that only use SSL/TLS are not impacted by this issue. Fixed in OpenSSL 3.0.6 (Affected 3.0.0-3.0.5). (CVE-2022-3358)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-3358

http://www.nessus.org/u?ca4894f6

https://www.openssl.org/news/secadv/20221011.txt

### Solution

Upgrade to OpenSSL version 3.0.6 or later.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-3358 |
| XREF | IAVA:2022-A-0415-S |

Plugin Information

Published: 2022/10/11, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.6
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.6
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.6
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.6
```

## 166773 - OpenSSL 3.0.0 < 3.0.7 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.7. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.7 advisory.

- A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. (CVE-2022-3786)

- A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server.

In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). (CVE-2022-3602)

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://www.openssl.org/news/secadv/20221101.txt

http://www.nessus.org/u?b279f369

http://www.nessus.org/u?ba8a3e9f

https://www.cve.org/CVERecord?id=CVE-2022-3602

https://www.cve.org/CVERecord?id=CVE-2022-3786

### Solution

Upgrade to OpenSSL version 3.0.7 or later.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.1016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-3602 |
| CVE | CVE-2022-3786 |
| XREF | IAVA:2022-A-0452-S |
| XREF | CEA-ID:CEA-2022-0036 |

Plugin Information

Published: 2022/11/01, Modified: 2024/06/07

Plugin Output

tcp/0

```
Path              : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
Reported version : 3.0.2
Fixed version     : 3.0.7
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.7
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.7
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.7
```

## 168829 - OpenSSL 3.0.0 < 3.0.8 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.8. It is, therefore, affected by a denial of service (DoS) vulnerability. If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the -policy argument to the command line utilities or by calling either X509_VERIFY_PARAM_add0_policy() or X509_VERIFY_PARAM_set1_policies() functions.

- There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName.

X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network. (CVE-2023-0286)

- If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the

`-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()'

function. Update (31 March 2023): The description of the policy processing enablement was corrected based on CVE-2023-0466. (CVE-2022-3996)

- A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. The read buffer overrun might result in a crash which could lead to a denial of service attack. In theory it could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext) although we are not aware of any working exploit leading to memory contents disclosure as of the time of release of this advisory. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. (CVE-2022-4203)

- A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption.

The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number

of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection. (CVE-2022-4304)

- The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the name (e.g.

CERTIFICATE), any header data and the payload data. If the function succeeds then the name_out, header and data arguments are populated with pointers to buffers containing the relevant decoded data.

The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue. (CVE-2022-4450)

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://www.cve.org/CVERecord?id=CVE-2023-0401

https://www.openssl.org/news/secadv/20230207.txt

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

https://www.cve.org/CVERecord?id=CVE-2023-0286

https://www.cve.org/CVERecord?id=CVE-2023-0217

https://www.cve.org/CVERecord?id=CVE-2023-0216

https://www.cve.org/CVERecord?id=CVE-2023-0215

https://www.cve.org/CVERecord?id=CVE-2022-4450

https://www.cve.org/CVERecord?id=CVE-2022-4304

https://www.cve.org/CVERecord?id=CVE-2022-4203

## Solution

Upgrade to OpenSSL version 3.0.8 or later.

## 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:N/A:H)

## CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0049

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-3996 |
| CVE | CVE-2022-4203 |
| CVE | CVE-2022-4304 |
| CVE | CVE-2022-4450 |
| CVE | CVE-2023-0215 |
| CVE | CVE-2023-0216 |
| CVE | CVE-2023-0217 |
| CVE | CVE-2023-0286 |
| CVE | CVE-2023-0401 |
| XREF | IAVA:2022-A-0518-S |

Plugin Information

Published: 2022/12/15, Modified: 2024/01/08

Plugin Output

tcp/0

```
Path              : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
Reported version : 3.0.2
Fixed version     : 3.0.8
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

## 183890 - OpenSSL 3.1.0 < 3.1.4 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.4. It is, therefore, affected by a vulnerability as referenced in the 3.1.4 advisory.

- Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths.

This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers.

Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the keylen parameter or the IV length, via the ivlen parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.

(CVE-2023-5363)

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

### See Also

http://www.nessus.org/u?442518e0

https://www.cve.org/CVERecord?id=CVE-2023-5363

https://www.openssl.org/news/secadv/20231024.txt

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

### Solution

Upgrade to OpenSSL version 3.1.4 or later.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5363 |
| XREF | IAVA:2023-A-0582-S |

Plugin Information

Published: 2023/10/25, Modified: 2024/03/08

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/2bbb5ec3fdcf5666e9849822366e5d09a7a4c0aa114e6f17d554f73ea9356d1c/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.4
```

## 205195 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos vulnerabilities (USN-6947-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6947-1 advisory.

It was discovered that Kerberos incorrectly handled GSS message tokens where an unwrapped token could appear to be truncated. An attacker could possibly use this issue to cause a denial of service.

(CVE-2024-37370)

It was discovered that Kerberos incorrectly handled GSS message tokens when sent a token with invalid length fields. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-37371)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6947-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.2

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2024-37370 |
| CVE | CVE-2024-37371 |
| XREF | USN:6947-1 |

### Plugin Information

Published: 2024/08/08, Modified: 2024/08/08

### Plugin Output

tcp/0

```
- Installed package : libgssapi-krb5-2_1.19.2-2ubuntu0.3
- Fixed package     : libgssapi-krb5-2_1.19.2-2ubuntu0.4

- Installed package : libk5crypto3_1.19.2-2ubuntu0.3
- Fixed package     : libk5crypto3_1.19.2-2ubuntu0.4

- Installed package : libkrb5-3_1.19.2-2ubuntu0.3
- Fixed package     : libkrb5-3_1.19.2-2ubuntu0.4

- Installed package : libkrb5support0_1.19.2-2ubuntu0.3
- Fixed package     : libkrb5support0_1.19.2-2ubuntu0.4
```

## 195216 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6768-1 advisory.

- An issue was discovered in GNOME GLib before 2.78.5, and 2.79.x and 2.80.x before 2.80.1. When a GDBus- based client subscribes to signals from a trusted system service such as NetworkManager on a shared computer, other users of the same computer can send spoofed D-Bus signals that the GDBus-based client will wrongly interpret as having been sent by the trusted system service. This could lead to the GDBus-based client behaving incorrectly, with an application-dependent impact. (CVE-2024-34397)

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

### See Also

https://ubuntu.com/security/notices/USN-6768-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

2.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2024-34397 |
| XREF | USN:6768-1 |

### Plugin Information

Published: 2024/05/09, Modified: 2024/05/09

### Plugin Output

tcp/0

```
  - Installed package : libglib2.0-data_2.72.4-0ubuntu2.2
  - Fixed package     : libglib2.0-data_2.72.4-0ubuntu2.3
```

## 203144 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Bind vulnerabilities (USN-6909-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6909-1 advisory.

It was discovered that Bind incorrectly handled a flood of DNS messages over TCP. A remote attacker could possibly use this issue to cause Bind to become unstable, resulting in a denial of service.

(CVE-2024-0760)

Toshifumi Sakaguchi discovered that Bind incorrectly handled having a very large number of RRs existing at the same time. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service. (CVE-2024-1737)

It was discovered that Bind incorrectly handled a large number of SIG(0) signed requests. A remote attacker could possibly use this issue to cause Bind to consume resources, leading to a denial of service.

(CVE-2024-1975)

Daniel Strnger discovered that Bind incorrectly handled serving both stable cache data and authoritative zone content. A remote attacker could possibly use this issue to cause Bind to crash, resulting in a denial of service. (CVE-2024-4076)

On Ubuntu 20.04 LTS, Bind has been updated from 9.16 to 9.18. In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Please see the following for more information:

https://kb.isc.org/docs/changes-to-be-aware-of-when-moving-from-bind-916-to-918

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6909-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0005

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2024-0760 |
| CVE | CVE-2024-1737 |
| CVE | CVE-2024-1975 |
| CVE | CVE-2024-4076 |
| XREF | USN:6909-1 |
| XREF | IAVA:2024-A-0442 |

Plugin Information

Published: 2024/07/23, Modified: 2024/07/26

Plugin Output

tcp/0

```
  - Installed package : bind9-dnsutils_1:9.18.24-0ubuntu0.22.04.1
  - Fixed package     : bind9-dnsutils_1:9.18.28-0ubuntu0.22.04.1

  - Installed package : bind9-host_1:9.18.24-0ubuntu0.22.04.1
  - Fixed package     : bind9-host_1:9.18.28-0ubuntu0.22.04.1
```

```
  - Installed package : bind9-libs_1:9.18.24-0ubuntu0.22.04.1
  - Fixed package     : bind9-libs_1:9.18.28-0ubuntu0.22.04.1
```

## 204989 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-6944-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6944-1 advisory.

Dov Murik discovered that curl incorrectly handled parsing ASN.1 Generalized Time fields. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly obtain sensitive memory contents.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-6944-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.9

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### STIG Severity

I

### References

| | |
|---|---|
| CVE | CVE-2024-7264 |
| XREF | IAVA:2024-A-0457 |
| XREF | USN:6944-1 |

### Plugin Information

Published: 2024/08/05, Modified: 2024/08/05

### Plugin Output

tcp/0

```
- Installed package : curl_7.81.0-1ubuntu1.16
- Fixed package     : curl_7.81.0-1ubuntu1.17

- Installed package : libcurl3-gnutls_7.81.0-1ubuntu1.16
- Fixed package     : libcurl3-gnutls_7.81.0-1ubuntu1.17

- Installed package : libcurl4_7.81.0-1ubuntu1.16
- Fixed package     : libcurl4_7.81.0-1ubuntu1.17
```

## 186742 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6549-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6549-1 advisory.

- An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and crash in read_descriptors in drivers/usb/core/sysfs.c. (CVE-2023-37453)

- A flaw was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem). This issue may allow a malicious user with CAP_NET_ADMIN privileges to cause a 4 byte out-of-bounds read of XFRMA_MTIMER_THRESH when parsing netlink attributes, leading to potential leakage of sensitive heap data to userspace. (CVE-2023-3773)

- A flaw was found in the Netfilter subsystem in the Linux kernel. The nfnl_osf_add_callback function did not validate the user mode controlled opt_num field. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure. (CVE-2023-39189)

- A flaw was found in the Netfilter subsystem in the Linux kernel. The xt_u32 module did not validate the fields in the xt_u32 structure. This flaw allows a local privileged attacker to trigger an out-of-bounds read by setting the size fields with a value beyond the array boundaries, leading to a crash or information disclosure. (CVE-2023-39192)

- A flaw was found in the Netfilter subsystem in the Linux kernel. The sctp_mt_check did not validate the flag_count field. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure. (CVE-2023-39193)

- A flaw was found in the XFRM subsystem in the Linux kernel. The specific flaw exists within the processing of state filters, which can result in a read past the end of an allocated buffer. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, potentially leading to an information disclosure. (CVE-2023-39194)

- A race condition was found in the QXL driver in the Linux kernel. The qxl_mode_dumb_create() function dereferences the qobj returned by the qxl_gem_object_create_with_handle(), but the handle is the only one holding a reference to it. This flaw allows an attacker to guess the returned handle value and trigger a use-after-free issue, potentially leading to a denial of service or privilege escalation. (CVE-2023-39198)

- A NULL pointer dereference flaw was found in the Linux kernel ipv4 stack. The socket buffer (skb) was assumed to be associated with a device before calling __ip_options_compile, which is not always the case if the skb is re-routed by ipvs. This issue may allow a local user with CAP_NET_ADMIN privileges to crash the system. (CVE-2023-42754)

- A flaw was found in vringh_kiov_advance in drivers/vhost/vringh.c in the host side of a virtio ring in the Linux Kernel. This issue may result in a denial of service from guest to host via zero length descriptor.

(CVE-2023-5158)

- A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe-oF/TCP subsystem in the Linux kernel. This issue may allow a malicious local privileged user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation problem. (CVE-2023-5178)

- A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation. If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer. We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06. (CVE-2023-5717)

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://ubuntu.com/security/notices/USN-6549-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

## EPSS Score

0.0243

## CVSS v2.0 Base Score

9.0 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-3773 |
| CVE | CVE-2023-5158 |
| CVE | CVE-2023-5178 |

| | |
|---|---|
| CVE | CVE-2023-5717 |
| CVE | CVE-2023-37453 |
| CVE | CVE-2023-39189 |
| CVE | CVE-2023-39192 |
| CVE | CVE-2023-39193 |
| CVE | CVE-2023-39194 |
| CVE | CVE-2023-39198 |
| CVE | CVE-2023-42754 |
| XREF | USN:6549-1 |

## Plugin Information

Published: 2023/12/11, Modified: 2024/06/19

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-91-generic
 for this advisory.
```

## 189610 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6609-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6609-1 advisory.

- An out-of-bounds access vulnerability involving netfilter was reported and fixed as: f1082dd31fe4 (netfilter: nf_tables: Reject tables of unsupported family); While creating a new netfilter table, lack of a safeguard against invalid nf_tables family (pf) values within `nf_tables_newtable` function enables an attacker to achieve out-of-bounds access. (CVE-2023-6040)

- An out-of-bounds read vulnerability was found in smbCalcSize in fs/smb/client/netmisc.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information.

(CVE-2023-6606)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a. (CVE-2023-6817)

- A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation. A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group(). We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b. (CVE-2023-6931)

- A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation. A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread. We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1. (CVE-2023-6932)

- A use-after-free flaw was found in the netfilter subsystem of the Linux kernel. If the catchall element is garbage-collected when the pipapo set is removed, the element can be deactivated twice. This can cause a use-after-free issue on an NFT_CHAIN object or NFT_OBJECT object, allowing a local unprivileged user with CAP_NET_ADMIN capability to escalate their privileges on the system. (CVE-2024-0193)

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://ubuntu.com/security/notices/USN-6609-1

### Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-6040 |
| CVE | CVE-2023-6606 |
| CVE | CVE-2023-6817 |
| CVE | CVE-2023-6931 |
| CVE | CVE-2023-6932 |
| CVE | CVE-2024-0193 |
| XREF | USN:6609-1 |

Plugin Information

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

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-92-generic
 for this advisory.
```

## 190122 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6626-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6626-1 advisory.

- A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel. (CVE-2023-32250)

- A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_LOGOFF commands. The issue results from the lack of proper validation of a pointer prior to accessing it. An attacker can leverage this vulnerability to create a denial-of- service condition on the system. (CVE-2023-32252)

- A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP and SMB2_LOGOFF commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel. (CVE-2023-32257)

- Closing of an event channel in the Linux kernel can result in a deadlock. This happens when the close is being performed in parallel to an unrelated Xen console action and the handling of a Xen console interrupt in an unprivileged guest. The closing of an event channel is e.g. triggered by removal of a paravirtual device on the other side. As this action will cause console messages to be issued on the other side quite often, the chance of triggering the deadlock is not neglectable. Note that 32-bit Arm-guests are not affected, as the 32-bit Linux kernel on Arm doesn't use queued-RW-locks, which are required to trigger the issue (on Arm32 a waiting writer doesn't block further readers to get the lock). (CVE-2023-34324)

- An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in ravb_remove in drivers/net/ethernet/renesas/ravb_main.c. (CVE-2023-35827)

- An issue was discovered in the Linux kernel before 6.5.9, exploitable by local users with userspace access to MMIO registers. Incorrect access checking in the #VC handler and instruction emulation of the SEV-ES emulation of MMIO accesses could lead to arbitrary write access to kernel memory (and thus privilege escalation). This depends on a race condition through which userspace can replace an instruction before the #VC handler reads it. (CVE-2023-46813)

- A use-after-free flaw was found in lan78xx_disconnect in drivers/net/usb/lan78xx.c in the network sub-component, net/usb/lan78xx in the Linux Kernel. This flaw allows a local attacker to crash the system when the LAN78XX USB device detaches. (CVE-2023-6039)

- A null pointer dereference flaw was found in the Linux kernel API for the cryptographic algorithm scatterwalk functionality. This issue occurs when a user constructs a malicious packet with specific socket configuration, which could allow a local user to crash the system or escalate their privileges on the system. (CVE-2023-6176)

- A null pointer dereference vulnerability was found in nft_dynset_init() in net/netfilter/nft_dynset.c in nf_tables in the Linux kernel. This issue may allow a local attacker with CAP_NET_ADMIN user privilege to trigger a denial of service. (CVE-2023-6622)

- A denial of service vulnerability was found in tipc_crypto_key_revoke in net/tipc/crypto.c in the Linux kernel's TIPC subsystem. This flaw allows guests with local user privileges to trigger a deadlock and potentially crash the system. (CVE-2024-0641)

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://ubuntu.com/security/notices/USN-6626-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.7

### EPSS Score

0.0076

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2023-6039 |
| CVE | CVE-2023-6176 |
| CVE | CVE-2023-6622 |
| CVE | CVE-2023-32250 |

| | |
|---|---|
| CVE | CVE-2023-32252 |
| CVE | CVE-2023-32257 |
| CVE | CVE-2023-34324 |
| CVE | CVE-2023-35827 |
| CVE | CVE-2023-46813 |
| CVE | CVE-2024-0641 |
| XREF | USN:6626-1 |

## Plugin Information

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

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-94-generic
 for this advisory.
```

## 190943 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6653-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6653-1 advisory.

- An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl in net/atm/ioctl.c has a use-after-free because of a vcc_recvmsg race condition. (CVE-2023-51780)

- An issue was discovered in the Linux kernel before 6.6.8. atalk_ioctl in net/appletalk/ddp.c has a use-after-free because of an atalk_recvmsg race condition. (CVE-2023-51781)

- A Null pointer dereference problem was found in ida_free in lib/idr.c in the Linux Kernel. This issue may allow an attacker using this library to cause a denial of service problem due to a missing check at a function return. (CVE-2023-6915)

- An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memcpy length, leading to a denial of service. (CVE-2024-0565)

- An out-of-bounds memory write flaw was found in the Linux kernel's Transport Layer Security functionality in how a user calls a function splice with a ktls socket as the destination. This flaw allows a local user to crash or potentially escalate their privileges on the system. (CVE-2024-0646)

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://ubuntu.com/security/notices/USN-6653-1

### Solution

Update the affected kernel package.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

7.7 (CVSS2#AV:A/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-51780 |
| CVE | CVE-2023-51781 |
| CVE | CVE-2023-6915 |
| CVE | CVE-2024-0565 |
| CVE | CVE-2024-0646 |
| XREF | USN:6653-1 |

Plugin Information

Published: 2024/02/23, Modified: 2024/03/11

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-97-generic
 for this advisory.
```

## 191737 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6686-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6686-1 advisory.

- In the Linux kernel before 5.17, an error path in dwc3_qcom_acpi_register_core in drivers/usb/dwc3/dwc3-qcom.c lacks certain platform_device_put and kfree calls. (CVE-2023-22995)

- In the Linux kernel before 6.5.9, there is a NULL pointer dereference in send_acknowledge in net/nfc/nci/spi.c. (CVE-2023-46343)

- An issue was discovered in the Linux kernel through 6.5.9. During a race with SQ thread exit, an io_uring/fdinfo.c io_uring_show_fdinfo NULL pointer dereference can occur. (CVE-2023-46862)

- bt_sock_recvmsg in net/bluetooth/af_bluetooth.c in the Linux kernel through 6.6.8 has a use-after-free because of a bt_sock_ioctl race condition. (CVE-2023-51779)

- An issue was discovered in the Linux kernel before 6.6.8. rose_ioctl in net/rose/af_rose.c has a use- after-free because of a rose_accept race condition. (CVE-2023-51782)

- An out-of-bounds read vulnerability was found in the NVMe-oF/TCP subsystem in the Linux kernel. This issue may allow a remote attacker to send a crafted TCP packet, triggering a heap-based buffer overflow that results in kmalloc data being printed and potentially leaked to the kernel ring buffer (dmesg).

(CVE-2023-6121)

- A vulnerability was found in vhost_new_msg in drivers/vhost/vhost.c in the Linux kernel, which does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This issue can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file. (CVE-2024-0340)

- A flaw was found in the Netfilter subsystem in the Linux kernel. The issue is in the nft_byteorder_eval() function, where the code iterates through a loop and writes to the `dst` array. On each iteration, 8 bytes are written, but `dst` is an array of u32, so each element only has space for 4 bytes. That means every iteration overwrites part of the previous element corrupting this array of u32. This flaw allows a local user to cause a denial of service or potentially break NetFilter functionality. (CVE-2024-0607)

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://ubuntu.com/security/notices/USN-6686-1

### Solution

Update the affected kernel package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0027

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-4134 |
| CVE | CVE-2023-6121 |
| CVE | CVE-2023-22995 |
| CVE | CVE-2023-46343 |
| CVE | CVE-2023-46862 |
| CVE | CVE-2023-51779 |
| CVE | CVE-2023-51782 |
| CVE | CVE-2024-0340 |
| CVE | CVE-2024-0607 |
| XREF | USN:6686-1 |

Plugin Information

Published: 2024/03/08, Modified: 2024/03/08

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-100-
generic for this advisory.
```

## 192312 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6704-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6704-1 advisory.

- In the Linux kernel before 5.17, drivers/phy/tegra/xusb.c mishandles the tegra_xusb_find_port_node return value. Callers expect NULL in the error case, but an error pointer is used. (CVE-2023-23000)

- A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the handling of SMB2_SESSION_SETUP commands. The issue results from the lack of control of resource consumption. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. (CVE-2023-32247)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The nft_setelem_catchall_deactivate() function checks whether the catch-all set element is active in the current generation instead of the next generation before freeing it, but only flags it inactive in the next generation, making it possible to free the element multiple times, leading to a double free vulnerability. We recommend upgrading past commit b1db244ffd041a49ecc9618e8feb6b5c1afcdaa7. (CVE-2024-1085)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The nft_verdict_init() function allows positive values as drop error within the hook verdict, and hence the nf_hook_slow() function can cause a double free vulnerability when NF_DROP is issued with a drop error which resembles NF_ACCEPT. We recommend upgrading past commit f342de4e2f33e0e39165d8639387aa6c19dff660. (CVE-2024-1086)

- A race condition was found in the Linux kernel's scsi device driver in lpfc_unregister_fcf_rescan() function. This can result in a null pointer dereference issue, possibly leading to a kernel panic or denial of service issue. (CVE-2024-24855)

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://ubuntu.com/security/notices/USN-6704-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

7.5 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.6

EPSS Score

0.0073

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

5.9 (CVSS2#E:H/RL:OF/RC:C)

References

| | |
|---|---|
| CVE | CVE-2023-23000 |
| CVE | CVE-2023-32247 |
| CVE | CVE-2024-1085 |
| CVE | CVE-2024-1086 |
| CVE | CVE-2024-24855 |
| XREF | USN:6704-1 |
| XREF | CISA-KNOWN-EXPLOITED:2024/06/20 |

Plugin Information

Published: 2024/03/20, Modified: 2024/05/30

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-101-
generic for this advisory.
```

## 193595 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6742-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6742-1 advisory.

- Bluetooth BR/EDR devices with Secure Simple Pairing and Secure Connections pairing in Bluetooth Core Specification 4.2 through 5.4 allow certain man-in-the-middle attacks that force a short key length, and might lead to discovery of the encryption key and live injection, aka BLUFFS. (CVE-2023-24023)

- In the Linux kernel, the following vulnerability has been resolved: jfs: fix uaf in jfs_evict_inode When the execution of diMount(ipimap) fails, the object ipimap that has been released may be accessed in diFreeSpecial(). Asynchronous ipimap release occurs when rcu_core() calls jfs_free_node(). Therefore, when diMount(ipimap) fails, sbi->ipimap should not be initialized as ipimap. (CVE-2023-52600)

- In the Linux kernel, the following vulnerability has been resolved: UBSAN: array-index-out-of-bounds in dtSplitRoot Syzkaller reported the following issue: oop0: detected capacity change from 0 to 32768 UBSAN:

array-index-out-of-bounds in fs/jfs/jfs_dtree.c:1971:9 index -2 is out of range for type 'struct dtslot [128]' CPU: 0 PID: 3613 Comm: syz-executor270 Not tainted 6.0.0-syzkaller-09423-g493ffd6605b2 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/22/2022 Call Trace: <TASK>

__dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x1b1/0x28e lib/dump_stack.c:106 ubsan_epilogue lib/ubsan.c:151 [inline] __ubsan_handle_out_of_bounds+0xdb/0x130 lib/ubsan.c:283 dtSplitRoot+0x8d8/0x1900 fs/jfs/jfs_dtree.c:1971 dtSplitUp fs/jfs/jfs_dtree.c:985 [inline] dtInsert +0x1189/0x6b80 fs/jfs/jfs_dtree.c:863 jfs_mkdir+0x757/0xb00 fs/jfs/namei.c:270 vfs_mkdir+0x3b3/0x590 fs/namei.c:4013 do_mkdirat+0x279/0x550 fs/namei.c:4038 __do_sys_mkdirat fs/namei.c:4053 [inline] __se_sys_mkdirat fs/namei.c:4051 [inline] __x64_sys_mkdirat+0x85/0x90 fs/namei.c:4051 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x3d/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7fcdc0113fd9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 c0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffeb8bc67d8 EFLAGS: 00000246 ORIG_RAX: 0000000000000102 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007fcdc0113fd9 RDX:

0000000000000000 RSI: 0000000020000340 RDI: 0000000000000003 RBP: 00007fcdc00d37a0 R08: 0000000000000000 R09: 00007fcdc00d37a0 R10: 00005555559a72c0 R11: 0000000000000246 R12: 00000000f8008000 R13:

0000000000000000 R14: 00083878000000f8 R15: 0000000000000000 </TASK> The issue is caused when the value of fsi becomes less than -1. The check to break the loop when fsi value becomes -1 is present but syzbot was able to produce value less than -1 which cause the error. This patch simply add the change for the values less than 0. The patch is tested via syzbot. (CVE-2023-52603)

- In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_rbtree: skip end interval element from gc rbtree lazy gc on insert might collect an end interval element that has been just added in this transactions, skip end interval elements that are not yet active. (CVE-2024-26581)

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://ubuntu.com/security/notices/USN-6742-1

## Solution

Update the affected kernel package.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.7

## EPSS Score

0.0033

## CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-24023 |
| CVE | CVE-2023-52600 |
| CVE | CVE-2023-52603 |
| CVE | CVE-2024-26581 |
| XREF | USN:6742-1 |

## Plugin Information

Published: 2024/04/19, Modified: 2024/04/19

## Plugin Output

### tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-105-
generic for this advisory.
```

## 195134 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6766-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6766-1 advisory.

- In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix UAF issue in ksmbd_tcp_new_connection() The race is between the handling of a new TCP connection and its disconnection. It leads to UAF on `struct tcp_transport` in ksmbd_tcp_new_connection() function.

(CVE-2024-26592)

- In the Linux kernel, the following vulnerability has been resolved: i2c: i801: Fix block process call transactions According to the Intel datasheets, software must reset the block buffer index twice for block process call transactions: once before writing the outgoing data to the buffer, and once again before reading the incoming data from the buffer. The driver is currently missing the second reset, causing the wrong portion of the block buffer to be read. (CVE-2024-26593)

- In the Linux kernel, the following vulnerability has been resolved:

ksmbd: validate mech token in session setup If client send invalid mech token in session setup request, ksmbd validate and make the error if it is invalid. (CVE-2024-26594)

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://ubuntu.com/security/notices/USN-6766-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

EPSS Score

0.0005

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-52435 |
| CVE | CVE-2023-52486 |
| CVE | CVE-2023-52489 |
| CVE | CVE-2023-52491 |
| CVE | CVE-2023-52492 |
| CVE | CVE-2023-52493 |
| CVE | CVE-2023-52494 |
| CVE | CVE-2023-52498 |
| CVE | CVE-2023-52583 |
| CVE | CVE-2023-52587 |
| CVE | CVE-2023-52588 |
| CVE | CVE-2023-52594 |
| CVE | CVE-2023-52595 |
| CVE | CVE-2023-52597 |
| CVE | CVE-2023-52598 |
| CVE | CVE-2023-52599 |
| CVE | CVE-2023-52601 |
| CVE | CVE-2023-52602 |
| CVE | CVE-2023-52604 |
| CVE | CVE-2023-52606 |
| CVE | CVE-2023-52607 |
| CVE | CVE-2023-52608 |
| CVE | CVE-2023-52614 |
| CVE | CVE-2023-52615 |
| CVE | CVE-2023-52616 |
| CVE | CVE-2023-52617 |
| CVE | CVE-2023-52618 |
| CVE | CVE-2023-52619 |
| CVE | CVE-2023-52622 |

| | |
|---|---|
| CVE | CVE-2023-52623 |
| CVE | CVE-2023-52627 |
| CVE | CVE-2023-52631 |
| CVE | CVE-2023-52633 |
| CVE | CVE-2023-52635 |
| CVE | CVE-2023-52637 |
| CVE | CVE-2023-52638 |
| CVE | CVE-2023-52642 |
| CVE | CVE-2023-52643 |
| CVE | CVE-2024-1151 |
| CVE | CVE-2024-2201 |
| CVE | CVE-2024-23849 |
| CVE | CVE-2024-26592 |
| CVE | CVE-2024-26593 |
| CVE | CVE-2024-26594 |
| CVE | CVE-2024-26600 |
| CVE | CVE-2024-26602 |
| CVE | CVE-2024-26606 |
| CVE | CVE-2024-26608 |
| CVE | CVE-2024-26610 |
| CVE | CVE-2024-26614 |
| CVE | CVE-2024-26615 |
| CVE | CVE-2024-26625 |
| CVE | CVE-2024-26627 |
| CVE | CVE-2024-26635 |
| CVE | CVE-2024-26636 |
| CVE | CVE-2024-26640 |
| CVE | CVE-2024-26641 |
| CVE | CVE-2024-26644 |
| CVE | CVE-2024-26645 |
| CVE | CVE-2024-26660 |
| CVE | CVE-2024-26663 |
| CVE | CVE-2024-26664 |
| CVE | CVE-2024-26665 |
| CVE | CVE-2024-26668 |
| CVE | CVE-2024-26671 |
| CVE | CVE-2024-26673 |
| CVE | CVE-2024-26675 |
| CVE | CVE-2024-26676 |
| CVE | CVE-2024-26679 |
| CVE | CVE-2024-26684 |
| CVE | CVE-2024-26685 |
| CVE | CVE-2024-26689 |

| | |
|---|---|
| CVE | CVE-2024-26695 |
| CVE | CVE-2024-26696 |
| CVE | CVE-2024-26697 |
| CVE | CVE-2024-26698 |
| CVE | CVE-2024-26702 |
| CVE | CVE-2024-26704 |
| CVE | CVE-2024-26707 |
| CVE | CVE-2024-26712 |
| CVE | CVE-2024-26715 |
| CVE | CVE-2024-26717 |
| CVE | CVE-2024-26720 |
| CVE | CVE-2024-26722 |
| CVE | CVE-2024-26808 |
| CVE | CVE-2024-26825 |
| CVE | CVE-2024-26826 |
| CVE | CVE-2024-26829 |
| CVE | CVE-2024-26910 |
| CVE | CVE-2024-26916 |
| CVE | CVE-2024-26920 |
| XREF | USN:6766-1 |

## Plugin Information

Published: 2024/05/07, Modified: 2024/06/24

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-106-
generic for this advisory.
```

## 200223 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6820-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6820-1 advisory.

It was discovered that the ATA over Ethernet (AoE) driver in the Linux kernel contained a race condition, leading to a use-after-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. (CVE-2023-6270)

It was discovered that the Atheros 802.11ac wireless driver did not properly validate certain data structures, leading to a NULL pointer dereference. An attacker could possibly use this to cause a denial of service. (CVE-2023-7042)

It was discovered that the HugeTLB file system component of the Linux Kernel contained a NULL pointer dereference vulnerability. A privileged attacker could possibly use this to to cause a denial of service.

(CVE-2024-0841)

It was discovered that the Intel Data Streaming and Intel Analytics Accelerator drivers in the Linux kernel allowed direct access to the devices for unprivileged users and virtual machines. A local attacker could use this to cause a denial of service. (CVE-2024-21823)

Yuxuan Hu discovered that the Bluetooth RFCOMM protocol driver in the Linux Kernel contained a race condition, leading to a NULL pointer dereference. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-22099)

It was discovered that the MediaTek SoC Gigabit Ethernet driver in the Linux kernel contained a race condition when stopping the device. A local attacker could possibly use this to cause a denial of service (device unavailability). (CVE-2024-27432)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM32 architecture;

- RISC-V architecture;

- x86 architecture;

- ACPI drivers;

- Block layer subsystem;

- Clock framework and drivers;

- CPU frequency scaling framework;

- Cryptographic API;

- DMA engine subsystem;

- EFI core;

- GPU drivers;
- InfiniBand drivers;
- IOMMU subsystem;
- Multiple devices driver;
- Media drivers;
- MMC subsystem;
- Network drivers;
- NTB driver;
- NVME drivers;
- PCI subsystem;
- MediaTek PM domains;
- Power supply drivers;
- SPI subsystem;
- Media staging drivers;
- TCM subsystem;
- USB subsystem;
- Framebuffer layer;
- AFS file system;
- File systems infrastructure;
- BTRFS file system;
- EROFS file system;
- Ext4 file system;
- F2FS file system;
- Network file system client;
- NTFS3 file system;
- Diskquota system;
- SMB network file system;
- BPF subsystem;
- Netfilter;
- TLS protocol;
- io_uring subsystem;

- Bluetooth subsystem;

- Memory management;

- Ethernet bridge;

- Networking core;

- HSR network protocol;

- IPv4 networking;

- IPv6 networking;

- L2TP protocol;

- MAC80211 subsystem;

- Multipath TCP;

- Netlink;

- NET/ROM layer;

- Packet sockets;

- RDS protocol;

- Sun RPC protocol;

- Unix domain sockets;

- Wireless networking;

- USB sound devices; (CVE-2024-26776, CVE-2024-26802, CVE-2024-26790, CVE-2024-27388, CVE-2024-27077, CVE-2024-26884, CVE-2024-26779, CVE-2024-26897, CVE-2024-27045, CVE-2024-26851, CVE-2024-27065, CVE-2024-26843, CVE-2024-26743, CVE-2024-27052, CVE-2024-26855, CVE-2024-27436, CVE-2024-27078, CVE-2024-26898, CVE-2024-27405, CVE-2024-26894, CVE-2024-26584, CVE-2024-26915, CVE-2024-26763, CVE-2024-27047, CVE-2024-26809, CVE-2024-26883, CVE-2024-26901, CVE-2024-27412, CVE-2024-26803, CVE-2024-26751, CVE-2024-35829, CVE-2024-27432, CVE-2023-52447, CVE-2024-26748, CVE-2024-27051, CVE-2023-52434, CVE-2024-26749, CVE-2024-27034, CVE-2024-27390, CVE-2024-26879, CVE-2024-26859, CVE-2024-26835, CVE-2024-26861, CVE-2024-27030, CVE-2024-27415, CVE-2023-52656, CVE-2024-26773, CVE-2024-27043, CVE-2024-26601, CVE-2024-27073, CVE-2024-26782, CVE-2024-27413, CVE-2024-26880, CVE-2024-26793, CVE-2024-26766, CVE-2024-26750, CVE-2024-26852, CVE-2024-26805, CVE-2024-35830, CVE-2024-26798, CVE-2023-52644, CVE-2024-26787, CVE-2024-26846, CVE-2024-26857, CVE-2024-26752, CVE-2024-26792, CVE-2023-52641, CVE-2024-26771, CVE-2024-26736, CVE-2024-27417, CVE-2024-26840, CVE-2024-26838, CVE-2024-26820, CVE-2024-26778, CVE-2024-26688, CVE-2024-27403, CVE-2024-26862, CVE-2024-27038, CVE-2024-26839, CVE-2024-26889, CVE-2024-26774, CVE-2024-26907, CVE-2023-52645, CVE-2024-27431, CVE-2024-27410, CVE-2024-27416, CVE-2024-26795, CVE-2023-52497, CVE-2024-27419, CVE-2024-26744, CVE-2024-26833, CVE-2024-26735, CVE-2024-26651, CVE-2024-27074, CVE-2023-52652, CVE-2024-27044, CVE-2024-26733, CVE-2024-26659, CVE-2024-35811, CVE-2024-27053, CVE-2024-27037, CVE-2023-52620, CVE-2024-26882, CVE-2024-35828, CVE-2024-26856, CVE-2024-26881, CVE-2024-27075, CVE-2024-26583, CVE-2023-52662, CVE-2024-26788, CVE-2024-26903, CVE-2024-26870, CVE-2024-26777, CVE-2024-26874, CVE-2024-26906, CVE-2024-26872, CVE-2024-26895, CVE-2024-26845, CVE-2024-27024, CVE-2024-27076, CVE-2024-26603, CVE-2024-27054, CVE-2024-26754, CVE-2024-35844, CVE-2024-26764, CVE-2024-26885, CVE-2024-26772, CVE-2024-26804, CVE-2024-26585, CVE-2024-26791, CVE-2024-27414, CVE-2024-26878, CVE-2024-26816, CVE-2024-27046, CVE-2024-26891, CVE-2024-26875,

CVE-2024-26747, CVE-2024-26863, CVE-2023-52640, CVE-2023-52650, CVE-2024-27039, CVE-2024-26877, CVE-2024-26801, CVE-2024-35845, CVE-2024-26769, CVE-2024-27028, CVE-2024-26737)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6820-1

## Solution

Update the affected kernel package.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

## EPSS Score

0.0004

## CVSS v2.0 Base Score

7.7 (CVSS2#AV:A/AC:L/Au:S/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-6270 |
| CVE | CVE-2023-7042 |
| CVE | CVE-2023-52434 |

| | |
|---|---|
| CVE | CVE-2023-52447 |
| CVE | CVE-2023-52497 |
| CVE | CVE-2023-52620 |
| CVE | CVE-2023-52640 |
| CVE | CVE-2023-52641 |
| CVE | CVE-2023-52644 |
| CVE | CVE-2023-52645 |
| CVE | CVE-2023-52650 |
| CVE | CVE-2023-52652 |
| CVE | CVE-2023-52656 |
| CVE | CVE-2023-52662 |
| CVE | CVE-2024-0841 |
| CVE | CVE-2024-21823 |
| CVE | CVE-2024-22099 |
| CVE | CVE-2024-26583 |
| CVE | CVE-2024-26584 |
| CVE | CVE-2024-26585 |
| CVE | CVE-2024-26601 |
| CVE | CVE-2024-26603 |
| CVE | CVE-2024-26651 |
| CVE | CVE-2024-26659 |
| CVE | CVE-2024-26688 |
| CVE | CVE-2024-26733 |
| CVE | CVE-2024-26735 |
| CVE | CVE-2024-26736 |
| CVE | CVE-2024-26737 |
| CVE | CVE-2024-26743 |
| CVE | CVE-2024-26744 |
| CVE | CVE-2024-26747 |
| CVE | CVE-2024-26748 |
| CVE | CVE-2024-26749 |
| CVE | CVE-2024-26750 |
| CVE | CVE-2024-26751 |
| CVE | CVE-2024-26752 |
| CVE | CVE-2024-26754 |
| CVE | CVE-2024-26763 |
| CVE | CVE-2024-26764 |
| CVE | CVE-2024-26766 |
| CVE | CVE-2024-26769 |
| CVE | CVE-2024-26771 |
| CVE | CVE-2024-26772 |
| CVE | CVE-2024-26773 |
| CVE | CVE-2024-26774 |

| | |
|---|---|
| CVE | CVE-2024-26776 |
| CVE | CVE-2024-26777 |
| CVE | CVE-2024-26778 |
| CVE | CVE-2024-26779 |
| CVE | CVE-2024-26782 |
| CVE | CVE-2024-26787 |
| CVE | CVE-2024-26788 |
| CVE | CVE-2024-26790 |
| CVE | CVE-2024-26791 |
| CVE | CVE-2024-26792 |
| CVE | CVE-2024-26793 |
| CVE | CVE-2024-26795 |
| CVE | CVE-2024-26798 |
| CVE | CVE-2024-26801 |
| CVE | CVE-2024-26802 |
| CVE | CVE-2024-26803 |
| CVE | CVE-2024-26804 |
| CVE | CVE-2024-26805 |
| CVE | CVE-2024-26809 |
| CVE | CVE-2024-26816 |
| CVE | CVE-2024-26820 |
| CVE | CVE-2024-26833 |
| CVE | CVE-2024-26835 |
| CVE | CVE-2024-26838 |
| CVE | CVE-2024-26839 |
| CVE | CVE-2024-26840 |
| CVE | CVE-2024-26843 |
| CVE | CVE-2024-26845 |
| CVE | CVE-2024-26846 |
| CVE | CVE-2024-26851 |
| CVE | CVE-2024-26852 |
| CVE | CVE-2024-26855 |
| CVE | CVE-2024-26856 |
| CVE | CVE-2024-26857 |
| CVE | CVE-2024-26859 |
| CVE | CVE-2024-26861 |
| CVE | CVE-2024-26862 |
| CVE | CVE-2024-26863 |
| CVE | CVE-2024-26870 |
| CVE | CVE-2024-26872 |
| CVE | CVE-2024-26874 |
| CVE | CVE-2024-26875 |
| CVE | CVE-2024-26877 |

| | |
|---|---|
| CVE | CVE-2024-26878 |
| CVE | CVE-2024-26879 |
| CVE | CVE-2024-26880 |
| CVE | CVE-2024-26881 |
| CVE | CVE-2024-26882 |
| CVE | CVE-2024-26883 |
| CVE | CVE-2024-26884 |
| CVE | CVE-2024-26885 |
| CVE | CVE-2024-26889 |
| CVE | CVE-2024-26891 |
| CVE | CVE-2024-26894 |
| CVE | CVE-2024-26895 |
| CVE | CVE-2024-26897 |
| CVE | CVE-2024-26898 |
| CVE | CVE-2024-26901 |
| CVE | CVE-2024-26903 |
| CVE | CVE-2024-26906 |
| CVE | CVE-2024-26907 |
| CVE | CVE-2024-26915 |
| CVE | CVE-2024-27024 |
| CVE | CVE-2024-27028 |
| CVE | CVE-2024-27030 |
| CVE | CVE-2024-27034 |
| CVE | CVE-2024-27037 |
| CVE | CVE-2024-27038 |
| CVE | CVE-2024-27039 |
| CVE | CVE-2024-27043 |
| CVE | CVE-2024-27044 |
| CVE | CVE-2024-27045 |
| CVE | CVE-2024-27046 |
| CVE | CVE-2024-27047 |
| CVE | CVE-2024-27051 |
| CVE | CVE-2024-27052 |
| CVE | CVE-2024-27053 |
| CVE | CVE-2024-27054 |
| CVE | CVE-2024-27065 |
| CVE | CVE-2024-27073 |
| CVE | CVE-2024-27074 |
| CVE | CVE-2024-27075 |
| CVE | CVE-2024-27076 |
| CVE | CVE-2024-27077 |
| CVE | CVE-2024-27078 |
| CVE | CVE-2024-27388 |

| | |
|---|---|
| CVE | CVE-2024-27390 |
| CVE | CVE-2024-27403 |
| CVE | CVE-2024-27405 |
| CVE | CVE-2024-27410 |
| CVE | CVE-2024-27412 |
| CVE | CVE-2024-27413 |
| CVE | CVE-2024-27414 |
| CVE | CVE-2024-27415 |
| CVE | CVE-2024-27416 |
| CVE | CVE-2024-27417 |
| CVE | CVE-2024-27419 |
| CVE | CVE-2024-27431 |
| CVE | CVE-2024-27432 |
| CVE | CVE-2024-27436 |
| CVE | CVE-2024-35811 |
| CVE | CVE-2024-35828 |
| CVE | CVE-2024-35829 |
| CVE | CVE-2024-35830 |
| CVE | CVE-2024-35844 |
| CVE | CVE-2024-35845 |
| XREF | USN:6820-1 |

## Plugin Information

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

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-112-
generic for this advisory.
```

## 202404 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6898-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6898-1 advisory.

Ziming Zhang discovered that the DRM driver for VMware Virtual GPU did not properly handle certain error conditions, leading to a NULL pointer dereference. A local attacker could possibly trigger this vulnerability to cause a denial of service. (CVE-2022-38096)

Gui-Dong Han discovered that the software RAID driver in the Linux kernel contained a race condition, leading to an integer overflow vulnerability. A privileged attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-23307)

It was discovered that a race condition existed in the Bluetooth subsystem in the Linux kernel when modifying certain settings values through debugfs. A privileged local attacker could use this to cause a denial of service. (CVE-2024-24857, CVE-2024-24858, CVE-2024-24859)

Bai Jiaju discovered that the Xceive XC4000 silicon tuner device driver in the Linux kernel contained a race condition, leading to an integer overflow vulnerability. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-24861)

Chenyuan Yang discovered that the Unsorted Block Images (UBI) flash device volume management subsystem did not properly validate logical eraseblock sizes in certain situations. An attacker could possibly use this to cause a denial of service (system crash). (CVE-2024-25739)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM64 architecture;

- RISC-V architecture;

- x86 architecture;

- Block layer subsystem;

- Accessibility subsystem;

- Android drivers;

- Bluetooth drivers;

- Clock framework and drivers;

- Data acquisition framework and drivers;

- Cryptographic API;

- DMA engine subsystem;

- GPU drivers;

- HID subsystem;
- I2C subsystem;
- IRQ chip drivers;
- Multiple devices driver;
- VMware VMCI Driver;
- MMC subsystem;
- Network drivers;
- Device tree and open firmware driver;
- PCI subsystem;
- S/390 drivers;
- SCSI drivers;
- Freescale SoC drivers;
- Trusted Execution Environment drivers;
- TTY drivers;
- USB subsystem;
- VFIO drivers;
- Framebuffer layer;
- Xen hypervisor drivers;
- File systems infrastructure;
- BTRFS file system;
- Ext4 file system;
- FAT file system;
- Network file system client;
- Network file system server daemon;
- NILFS2 file system;
- Pstore file system;
- SMB network file system;
- UBI file system;
- Netfilter;
- BPF subsystem;
- Core kernel;

- PCI iomap interfaces;

- Memory management;

- B.A.T.M.A.N. meshing protocol;

- Bluetooth subsystem;

- Ethernet bridge;

- Networking core;

- IPv4 networking;

- IPv6 networking;

- MAC80211 subsystem;

- IEEE 802.15.4 subsystem;

- NFC subsystem;

- Open vSwitch;

- RDS protocol;

- Network traffic control;

- SMC sockets;

- Unix domain sockets;

- eXpress Data Path;

- ALSA SH drivers;

- KVM core; (CVE-2024-35955, CVE-2024-35805, CVE-2024-26814, CVE-2024-27008, CVE-2024-26970, CVE-2024-35944, CVE-2024-27013, CVE-2024-35938, CVE-2024-35853, CVE-2024-35969, CVE-2024-26981, CVE-2024-26929, CVE-2024-27020, CVE-2024-35885, CVE-2024-35973, CVE-2024-35958, CVE-2024-26961, CVE-2024-35912, CVE-2024-35890, CVE-2024-35804, CVE-2024-35813, CVE-2024-27393, CVE-2024-26956, CVE-2024-35915, CVE-2024-26642, CVE-2024-35847, CVE-2024-26960, CVE-2024-26923, CVE-2024-35935, CVE-2024-36025, CVE-2024-35898, CVE-2024-26810, CVE-2024-35809, CVE-2024-26813, CVE-2024-36007, CVE-2024-35817, CVE-2024-35849, CVE-2024-35819, CVE-2024-35884, CVE-2024-35922, CVE-2024-36008, CVE-2024-27004, CVE-2024-35902, CVE-2024-26828, CVE-2024-35791, CVE-2024-35930, CVE-2024-26973, CVE-2024-26984, CVE-2024-35806, CVE-2024-26629, CVE-2024-26955, CVE-2024-26937, CVE-2024-27059, CVE-2024-35872, CVE-2024-35978, CVE-2024-26950, CVE-2024-27018, CVE-2024-35857, CVE-2024-35990, CVE-2024-27437, CVE-2024-35822, CVE-2024-36020, CVE-2024-26931, CVE-2024-26977, CVE-2024-26654, CVE-2024-26988, CVE-2024-36005, CVE-2024-26969, CVE-2024-35960, CVE-2024-27016, CVE-2024-36006, CVE-2024-35936, CVE-2024-35982, CVE-2024-36029, CVE-2024-27395, CVE-2024-26999, CVE-2024-35871, CVE-2024-35893, CVE-2024-26925, CVE-2024-26965, CVE-2024-35933, CVE-2024-35976, CVE-2024-35899, CVE-2024-35852, CVE-2024-35918, CVE-2024-26951, CVE-2024-27001, CVE-2024-35905, CVE-2024-35907, CVE-2024-26976, CVE-2024-27000, CVE-2024-35910, CVE-2024-35950, CVE-2024-26974, CVE-2024-35785, CVE-2023-52488, CVE-2023-52880, CVE-2024-35877, CVE-2024-35888, CVE-2024-35807, CVE-2024-35796, CVE-2024-35821, CVE-2024-35854, CVE-2024-27015, CVE-2024-35823, CVE-2024-35900, CVE-2024-35815, CVE-2024-26966, CVE-2024-26817, CVE-2024-35896, CVE-2024-27396, CVE-2024-27009, CVE-2024-35940, CVE-2024-26996, CVE-2024-35825, CVE-2024-35984, CVE-2024-35886, CVE-2024-27019, CVE-2024-26922, CVE-2024-35989, CVE-2024-26926, CVE-2024-35988, CVE-2024-26957, CVE-2024-26812, CVE-2024-35925, CVE-2024-35970, CVE-2024-26989, CVE-2024-26811, CVE-2024-35895, CVE-2024-26935, CVE-2024-26958, CVE-2024-35855, CVE-2024-35879, CVE-2024-26993, CVE-2024-35934, CVE-2024-36004, CVE-2024-35997,

CVE-2024-26994, CVE-2023-52699, CVE-2024-35789, CVE-2024-26964, CVE-2024-26687, CVE-2024-35851, CVE-2024-35897, CVE-2024-26934)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6898-1

## Solution

Update the affected kernel package.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

## EPSS Score

0.0004

## CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2022-38096 |
| CVE | CVE-2023-52488 |
| CVE | CVE-2023-52699 |

| | |
|---|---|
| CVE | CVE-2023-52880 |
| CVE | CVE-2024-23307 |
| CVE | CVE-2024-24857 |
| CVE | CVE-2024-24858 |
| CVE | CVE-2024-24859 |
| CVE | CVE-2024-24861 |
| CVE | CVE-2024-25739 |
| CVE | CVE-2024-26629 |
| CVE | CVE-2024-26642 |
| CVE | CVE-2024-26654 |
| CVE | CVE-2024-26687 |
| CVE | CVE-2024-26810 |
| CVE | CVE-2024-26811 |
| CVE | CVE-2024-26812 |
| CVE | CVE-2024-26813 |
| CVE | CVE-2024-26814 |
| CVE | CVE-2024-26817 |
| CVE | CVE-2024-26828 |
| CVE | CVE-2024-26922 |
| CVE | CVE-2024-26923 |
| CVE | CVE-2024-26925 |
| CVE | CVE-2024-26926 |
| CVE | CVE-2024-26929 |
| CVE | CVE-2024-26931 |
| CVE | CVE-2024-26934 |
| CVE | CVE-2024-26935 |
| CVE | CVE-2024-26937 |
| CVE | CVE-2024-26950 |
| CVE | CVE-2024-26951 |
| CVE | CVE-2024-26955 |
| CVE | CVE-2024-26956 |
| CVE | CVE-2024-26957 |
| CVE | CVE-2024-26958 |
| CVE | CVE-2024-26960 |
| CVE | CVE-2024-26961 |
| CVE | CVE-2024-26964 |
| CVE | CVE-2024-26965 |
| CVE | CVE-2024-26966 |
| CVE | CVE-2024-26969 |
| CVE | CVE-2024-26970 |
| CVE | CVE-2024-26973 |
| CVE | CVE-2024-26974 |
| CVE | CVE-2024-26976 |

| | |
|---|---|
| CVE | CVE-2024-26977 |
| CVE | CVE-2024-26981 |
| CVE | CVE-2024-26984 |
| CVE | CVE-2024-26988 |
| CVE | CVE-2024-26989 |
| CVE | CVE-2024-26993 |
| CVE | CVE-2024-26994 |
| CVE | CVE-2024-26996 |
| CVE | CVE-2024-26999 |
| CVE | CVE-2024-27000 |
| CVE | CVE-2024-27001 |
| CVE | CVE-2024-27004 |
| CVE | CVE-2024-27008 |
| CVE | CVE-2024-27009 |
| CVE | CVE-2024-27013 |
| CVE | CVE-2024-27015 |
| CVE | CVE-2024-27016 |
| CVE | CVE-2024-27018 |
| CVE | CVE-2024-27019 |
| CVE | CVE-2024-27020 |
| CVE | CVE-2024-27059 |
| CVE | CVE-2024-27393 |
| CVE | CVE-2024-27395 |
| CVE | CVE-2024-27396 |
| CVE | CVE-2024-27437 |
| CVE | CVE-2024-35785 |
| CVE | CVE-2024-35789 |
| CVE | CVE-2024-35791 |
| CVE | CVE-2024-35796 |
| CVE | CVE-2024-35804 |
| CVE | CVE-2024-35805 |
| CVE | CVE-2024-35806 |
| CVE | CVE-2024-35807 |
| CVE | CVE-2024-35809 |
| CVE | CVE-2024-35813 |
| CVE | CVE-2024-35815 |
| CVE | CVE-2024-35817 |
| CVE | CVE-2024-35819 |
| CVE | CVE-2024-35821 |
| CVE | CVE-2024-35822 |
| CVE | CVE-2024-35823 |
| CVE | CVE-2024-35825 |
| CVE | CVE-2024-35847 |

| | |
|---|---|
| CVE | CVE-2024-35849 |
| CVE | CVE-2024-35851 |
| CVE | CVE-2024-35852 |
| CVE | CVE-2024-35853 |
| CVE | CVE-2024-35854 |
| CVE | CVE-2024-35855 |
| CVE | CVE-2024-35857 |
| CVE | CVE-2024-35871 |
| CVE | CVE-2024-35872 |
| CVE | CVE-2024-35877 |
| CVE | CVE-2024-35879 |
| CVE | CVE-2024-35884 |
| CVE | CVE-2024-35885 |
| CVE | CVE-2024-35886 |
| CVE | CVE-2024-35888 |
| CVE | CVE-2024-35890 |
| CVE | CVE-2024-35893 |
| CVE | CVE-2024-35895 |
| CVE | CVE-2024-35896 |
| CVE | CVE-2024-35897 |
| CVE | CVE-2024-35898 |
| CVE | CVE-2024-35899 |
| CVE | CVE-2024-35900 |
| CVE | CVE-2024-35902 |
| CVE | CVE-2024-35905 |
| CVE | CVE-2024-35907 |
| CVE | CVE-2024-35910 |
| CVE | CVE-2024-35912 |
| CVE | CVE-2024-35915 |
| CVE | CVE-2024-35918 |
| CVE | CVE-2024-35922 |
| CVE | CVE-2024-35925 |
| CVE | CVE-2024-35930 |
| CVE | CVE-2024-35933 |
| CVE | CVE-2024-35934 |
| CVE | CVE-2024-35935 |
| CVE | CVE-2024-35936 |
| CVE | CVE-2024-35938 |
| CVE | CVE-2024-35940 |
| CVE | CVE-2024-35944 |
| CVE | CVE-2024-35950 |
| CVE | CVE-2024-35955 |
| CVE | CVE-2024-35958 |

| | |
|---|---|
| CVE | CVE-2024-35960 |
| CVE | CVE-2024-35969 |
| CVE | CVE-2024-35970 |
| CVE | CVE-2024-35973 |
| CVE | CVE-2024-35976 |
| CVE | CVE-2024-35978 |
| CVE | CVE-2024-35982 |
| CVE | CVE-2024-35984 |
| CVE | CVE-2024-35988 |
| CVE | CVE-2024-35989 |
| CVE | CVE-2024-35990 |
| CVE | CVE-2024-35997 |
| CVE | CVE-2024-36004 |
| CVE | CVE-2024-36005 |
| CVE | CVE-2024-36006 |
| CVE | CVE-2024-36007 |
| CVE | CVE-2024-36008 |
| CVE | CVE-2024-36020 |
| CVE | CVE-2024-36025 |
| CVE | CVE-2024-36029 |
| XREF | USN:6898-1 |

## Plugin Information

Published: 2024/07/15, Modified: 2024/07/19

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-116-
generic for this advisory.
```

## 204913 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6923-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6923-1 advisory.

Benedict Schlter, Supraja Sridhara, Andrin Bertschi, and Shweta Shinde discovered that an untrusted hypervisor could inject malicious #VC interrupts and compromise the security guarantees of AMD SEV-SNP.

This flaw is known as WeSee. A local attacker in control of the hypervisor could use this to expose sensitive information or possibly execute arbitrary code in the trusted execution environment.

(CVE-2024-25742)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- TTY drivers;

- SMB network file system;

- Netfilter;

- Bluetooth subsystem; (CVE-2024-26886, CVE-2024-26952, CVE-2023-52752, CVE-2024-27017, CVE-2024-36016)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6923-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-52752 |
| CVE | CVE-2024-25742 |
| CVE | CVE-2024-26886 |
| CVE | CVE-2024-26952 |
| CVE | CVE-2024-27017 |
| CVE | CVE-2024-36016 |
| XREF | USN:6923-1 |

Plugin Information

Published: 2024/07/31, Modified: 2024/07/31

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-117-
generic for this advisory.
```

## 189773 - Ubuntu 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-6616-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6616-1 advisory.

- A vulnerability was found in openldap. This security flaw causes a null pointer dereference in ber_memalloc_x() function. (CVE-2023-2953)

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

### See Also

https://ubuntu.com/security/notices/USN-6616-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0039

### CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-2953 |
| XREF | USN:6616-1 |

## Plugin Information

Published: 2024/01/30, Modified: 2024/01/30

## Plugin Output

tcp/0

```
  - Installed package : libldap-common_2.5.15+dfsg-0ubuntu0.22.04.1
  - Fixed package     : libldap-common_2.5.16+dfsg-0ubuntu0.22.04.2
```

## 204858 - Ubuntu 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-6928-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6928-1 advisory.

It was discovered that the Python ssl module contained a memory race condition when handling the APIs to obtain the CA certificates and certificate store statistics. This could possibly result in applications obtaining wrong results, leading to various SSL issues. (CVE-2024-0397)

It was discovered that the Python ipaddress module contained incorrect information about which IP address ranges were considered private or globally reachable. This could possibly result in applications applying incorrect security policies. (CVE-2024-4032)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6928-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.0

### EPSS Score

0.0005

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2024-0397 |
| CVE | CVE-2024-4032 |
| XREF | USN:6928-1 |

### Plugin Information

Published: 2024/07/30, Modified: 2024/07/30

### Plugin Output

tcp/0

```
- Installed package : libpython3.10_3.10.12-1~22.04.3
- Fixed package     : libpython3.10_3.10.12-1~22.04.5

- Installed package : libpython3.10-minimal_3.10.12-1~22.04.3
- Fixed package     : libpython3.10-minimal_3.10.12-1~22.04.5

- Installed package : libpython3.10-stdlib_3.10.12-1~22.04.3
- Fixed package     : libpython3.10-stdlib_3.10.12-1~22.04.5

- Installed package : python3.10_3.10.12-1~22.04.3
- Fixed package     : python3.10_3.10.12-1~22.04.5

- Installed package : python3.10-minimal_3.10.12-1~22.04.3
- Fixed package     : python3.10-minimal_3.10.12-1~22.04.5
```

## 50686 - IP Forwarding Enabled

### Synopsis

The remote host has IP forwarding enabled.

### Description

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

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

### Solution

On Linux, you can disable IP forwarding by doing :

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

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

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

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

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

For other systems, check with your vendor.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### VPR Score

4.0

### EPSS Score

0.0035

### CVSS v2.0 Base Score

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

### References

CVE CVE-1999-0511

## Plugin Information

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

## Plugin Output

tcp/0

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

 Detected local MAC Address        : 0050569480f8
 Response from local MAC Address   : 0050569480f8

 Detected Gateway MAC Address      : 3cecefde9d5e
 Response from Gateway MAC Address : 3cecefde9d5e
```

## 157228 - OpenSSL 1.1.1 < 1.1.1m Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc- dev (Affected 1.0.2-1.0.2zb). (CVE-2021-4160)

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

### See Also

http://www.nessus.org/u?da5b5058

https://www.cve.org/CVERecord?id=CVE-2021-4160

https://www.openssl.org/news/secadv/20220128.txt

### Solution

Upgrade to OpenSSL version 1.1.1m or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0042

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-4160

Plugin Information

Published: 2022/01/28, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

## 162721 - OpenSSL 1.1.1 < 1.1.1q Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of in place encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). (CVE-2022-2097)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-2097

http://www.nessus.org/u?ec8857b4

https://www.openssl.org/news/secadv/20220705.txt

### Solution

Upgrade to OpenSSL version 1.1.1q or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

2.2

### EPSS Score

0.0037

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-2097 |
| XREF | IAVA:2022-A-0265-S |

Plugin Information

Published: 2022/07/05, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

## 173260 - OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1u. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1u advisory.

- Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit.

OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(n^2) with 'n'

being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low. (CVE-2023-2650)

- Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0465)

- The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification.

As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable

the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument.

Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.

(CVE-2023-0466)

- A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0464)

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

## See Also

http://www.nessus.org/u?2b09deba

http://www.nessus.org/u?f976d208

https://www.openssl.org/news/secadv/20230328.txt

https://www.openssl.org/news/secadv/20230530.txt

https://www.openssl.org/policies/general/security-policy.html

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

http://www.nessus.org/u?1b17844f

http://www.nessus.org/u?0f79dd95

https://www.openssl.org/news/secadv/20230322.txt

https://www.cve.org/CVERecord?id=CVE-2023-0464

https://www.cve.org/CVERecord?id=CVE-2023-0464

https://www.cve.org/CVERecord?id=CVE-2023-0465

https://www.cve.org/CVERecord?id=CVE-2023-0466

https://www.cve.org/CVERecord?id=CVE-2023-2650

## Solution

Upgrade to OpenSSL version 1.1.1u or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.003

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0465 |
| CVE | CVE-2023-0466 |
| CVE | CVE-2023-2650 |
| XREF | IAVA:2023-A-0158-S |

Plugin Information

Published: 2023/03/22, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

## 178475 - OpenSSL 1.1.1 < 1.1.1v Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1v. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1v advisory.

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check().

Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the -check option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3817)

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3446)

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

### See Also

http://www.nessus.org/u?34493939

http://www.nessus.org/u?4c441c47

https://www.openssl.org/news/secadv/20230719.txt

https://www.openssl.org/news/secadv/20230731.txt

https://www.openssl.org/policies/secpolicy.html
https://www.cve.org/CVERecord?id=CVE-2023-3446
https://www.cve.org/CVERecord?id=CVE-2023-3817

## Solution

Upgrade to OpenSSL version 1.1.1v or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

2.2

## EPSS Score

0.0043

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-3446 |
| CVE | CVE-2023-3817 |
| XREF | IAVA:2023-A-0398-S |

## Plugin Information

Published: 2023/07/19, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

## 184811 - OpenSSL 1.1.1 < 1.1.1x Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

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

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

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

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

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

### See Also

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

https://www.cve.org/CVERecord?id=CVE-2024-0727

### Solution

Upgrade to OpenSSL version 1.1.1x or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5678 |
| CVE | CVE-2024-0727 |
| XREF | IAVA:2024-A-0121-S |

Plugin Information

Published: 2023/11/07, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9768992a25e6f6e963c9a3b5c4af5981944da49558318bb00e91f523ddfdd2df/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

## 192965 - OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1y. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1y advisory.

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4741

### Solution

Upgrade to OpenSSL version 1.1.1y or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### STIG Severity

I

### References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4741 |
| XREF | IAVA:2024-A-0208-S |

### Plugin Information

Published: 2024/04/08, Modified: 2024/06/07

### Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9768992a25e6f6e963c9a3b5c4af5981944da49558318bb00e91f523ddfdd2df/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

## 178478 - OpenSSL 3.0.0 < 3.0.10 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.10. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.10 advisory.

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3446)

- Issue summary: The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence. Impact summary: Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be mislead by removing adding or reordering such empty entries as these are ignored by the OpenSSL implementation. We are currently unaware of any such applications. The AES-SIV algorithm allows for authentication of multiple associated data entries along with the encryption. To authenticate empty data the application has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) with NULL pointer as the output buffer and 0 as the input buffer length. The AES-SIV implementation in OpenSSL just returns success for such a call instead of performing the associated data authentication operation. The empty data thus will not be authenticated. As this issue does not affect non-empty associated data authentication and we expect it to be rare for an application to use empty associated data entries this is qualified as Low severity issue. (CVE-2023-2975)

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

### See Also

http://www.nessus.org/u?92592957

http://www.nessus.org/u?e3173aec

https://www.openssl.org/news/secadv/20230719.txt

https://www.openssl.org/news/secadv/20230731.txt

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

http://www.nessus.org/u?a7b15686

https://www.openssl.org/news/secadv/20230714.txt
https://www.cve.org/CVERecord?id=CVE-2023-2975
https://www.cve.org/CVERecord?id=CVE-2023-3446
https://www.cve.org/CVERecord?id=CVE-2023-3817

## Solution

Upgrade to OpenSSL version 3.0.10 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

2.2

## EPSS Score

0.0043

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-2975 |
| CVE | CVE-2023-3446 |
| CVE | CVE-2023-3817 |
| XREF | IAVA:2023-A-0398-S |

## Plugin Information

Published: 2023/07/19, Modified: 2024/01/08

## Plugin Output

tcp/0

```
  Path             : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.10
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.10
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.10
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.10
```

## 185160 - OpenSSL 3.0.0 < 3.0.13 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.13. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.13 advisory.

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

- Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary:

Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2023-6237)

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

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

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

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

## See Also

http://www.nessus.org/u?02bfb3df

http://www.nessus.org/u?71a978e4

http://www.nessus.org/u?ccacbb1d

http://www.nessus.org/u?fc067b0a

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

https://www.cve.org/CVERecord?id=CVE-2023-6129

https://www.cve.org/CVERecord?id=CVE-2023-6237

https://www.cve.org/CVERecord?id=CVE-2024-0727

## Solution

Upgrade to OpenSSL version 3.0.13 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5678 |
| CVE | CVE-2023-6129 |
| CVE | CVE-2023-6237 |
| CVE | CVE-2024-0727 |
| XREF | IAVA:2024-A-0121-S |

Plugin Information

Published: 2023/11/07, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.13
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
```

```
  Fixed version    : 3.0.13
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.13
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.13
```

## 192966 - OpenSSL 3.0.0 < 3.0.14 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.14. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.14 advisory.

- Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary:

Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2024-4603)

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware

of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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

### See Also

http://www.nessus.org/u?141a6242

http://www.nessus.org/u?2cbb1fb1

http://www.nessus.org/u?8409be15

https://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4741

### Solution

Upgrade to OpenSSL version 3.0.14 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4603 |
| CVE | CVE-2024-4741 |
| XREF | IAVA:2024-A-0208-S |

## Plugin Information

Published: 2024/04/08, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path             : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.14
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.14
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.14
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.14
```

## 173263 - OpenSSL 3.0.0 < 3.0.9 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.9. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.9 advisory.

- The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification.

As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument.

Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.

(CVE-2023-0466)

- A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0464)

- Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0465)

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

### See Also

http://www.nessus.org/u?91a43679

https://www.cve.org/CVERecord?id=CVE-2023-0465

https://www.openssl.org/news/secadv/20230328.txt

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

http://www.nessus.org/u?a5af6e0b

https://www.cve.org/CVERecord?id=CVE-2023-0466

http://www.nessus.org/u?0fd4fada

https://www.cve.org/CVERecord?id=CVE-2023-0464
https://www.openssl.org/news/secadv/20230322.txt

## Solution

Upgrade to OpenSSL version 3.0.9 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

4.4

## EPSS Score

0.003

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0465 |
| CVE | CVE-2023-0466 |
| XREF | IAVA:2023-A-0158-S |

## Plugin Information

Published: 2023/03/22, Modified: 2024/01/08

## Plugin Output

tcp/0

```
  Path             : /run/initramfs/usr/lib/x86_64-linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/543c31155c158d36d1be461ae754244bd9ef19c064ab536c371b7ed21c2dd7dc/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

## 185161 - OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.5. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.5 advisory.

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

- Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary:

Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2023-6237)

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

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

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

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

## See Also

http://www.nessus.org/u?0a42ec4e

http://www.nessus.org/u?950a9188

http://www.nessus.org/u?aca829a1

http://www.nessus.org/u?d086a7ea

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

https://www.cve.org/CVERecord?id=CVE-2023-6129

https://www.cve.org/CVERecord?id=CVE-2023-6237

https://www.cve.org/CVERecord?id=CVE-2024-0727

## Solution

Upgrade to OpenSSL version 3.1.5 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5678 |
| CVE | CVE-2023-6129 |
| CVE | CVE-2023-6237 |
| CVE | CVE-2024-0727 |
| XREF | IAVA:2024-A-0121-S |

Plugin Information

Published: 2023/11/07, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/2bbb5ec3fdcf5666e9849822366e5d09a7a4c0aa114e6f17d554f73ea9356d1c/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.5
```

## 192974 - OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.6. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.6 advisory.

- Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary:

Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2024-4603)

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware

of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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

### See Also

http://www.nessus.org/u?5ee92eab

http://www.nessus.org/u?6f15218c

http://www.nessus.org/u?f40bd907

https://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4741

### Solution

Upgrade to OpenSSL version 3.1.6 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4603 |
| CVE | CVE-2024-4741 |
| XREF | IAVA:2024-A-0208-S |

## Plugin Information

Published: 2024/04/08, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/2bbb5ec3fdcf5666e9849822366e5d09a7a4c0aa114e6f17d554f73ea9356d1c/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.6
```

## 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/443/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=Caddy Local Authority - ECC Intermediate
|-Issuer  : CN=Caddy Local Authority - 2023 ECC Root
```

## 190598 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6640-1 advisory.

- A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.

(CVE-2023-4641)

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

### See Also

https://ubuntu.com/security/notices/USN-6640-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:C/I:N/A:N)

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2023-4641 |
| XREF | USN:6640-1 |

### Plugin Information

Published: 2024/02/15, Modified: 2024/02/15

### Plugin Output

tcp/0

```
  - Installed package : login_1:4.8.1-2ubuntu2.1
  - Fixed package     : login_1:4.8.1-2ubuntu2.2
```

## 185568 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-6478-1 advisory.

- In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines. (CVE-2023-46316)

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

### See Also

https://ubuntu.com/security/notices/USN-6478-1

### Solution

Update the affected traceroute package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-46316 |
| XREF | USN:6478-1 |

## Plugin Information

Published: 2023/11/14, Modified: 2024/01/23

## Plugin Output

tcp/0

```
  - Installed package : traceroute_1:2.1.0-2
  - Fixed package     : traceroute_1:2.1.0-2ubuntu0.22.04.1~esm1


NOTE: The fixed ESM package referenced in this plugin requires a
subscription to Ubuntu Pro to enable the ESM repositories.
```

## 193171 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : NSS vulnerabilities (USN-6727-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6727-1 advisory.

- The NSS code used for checking PKCS#1 v1.5 was leaking information useful in mounting Bleichenbacher-like attacks. Both the overall correctness of the padding as well as the length of the encrypted message was leaking through timing side-channel. By sending large number of attacker-selected ciphertexts, the attacker would be able to decrypt a previously intercepted PKCS#1 v1.5 ciphertext (for example, to decrypt a TLS session that used RSA key exchange), or forge a signature using the victim's key. The issue was fixed by implementing the implicit rejection algorithm, in which the NSS returns a deterministic random message in case invalid padding is detected, as proposed in the Marvin Attack paper. This vulnerability affects NSS < 3.61. (CVE-2023-4421)

- NSS was susceptible to a timing side-channel attack when performing RSA decryption. This attack could potentially allow an attacker to recover the private data. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9. (CVE-2023-5388)

- Multiple NSS NIST curves were susceptible to a side-channel attack known as Minerva. This attack could potentially allow an attacker to recover the private key. This vulnerability affects Firefox < 121.

(CVE-2023-6135)

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://ubuntu.com/security/notices/USN-6727-1

### Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0005

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:L/Au:S/C:C/I:N/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-4421 |
| CVE | CVE-2023-5388 |
| CVE | CVE-2023-6135 |
| XREF | USN:6727-1 |

Plugin Information

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

Plugin Output

tcp/0

```
- Installed package : libnss3_2:3.68.2-0ubuntu1.2
- Fixed package     : libnss3_2:3.98-0ubuntu0.22.04.1
```

## 203146 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : python-zipp vulnerability (USN-6906-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6906-1 advisory.

It was discovered that python-zipp did not properly handle the zip files with malformed names. An attacker could possibly use this issue to cause a denial of service.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-6906-1

### Solution

Update the affected pypy-zipp, python-zipp and / or python3-zipp packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2024-5569 |
| XREF | USN:6906-1 |

## Plugin Information

Published: 2024/07/23, Modified: 2024/07/24

## Plugin Output

tcp/0

```
  - Installed package : python3-zipp_1.0.0-3
  - Fixed package     : python3-zipp_1.0.0-3ubuntu0.1
```

## 184098 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6465-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6465-1 advisory.

- An issue was discovered in drivers/bluetooth/hci_ldisc.c in the Linux kernel 6.2. In hci_uart_tty_ioctl, there is a race condition between HCIUARTSETPROTO and HCIUARTGETPROTO. HCI_UART_PROTO_SET is set before hu->proto is set. A NULL pointer dereference may occur. (CVE-2023-31083)

- A flaw was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem). This issue may allow a malicious user with CAP_NET_ADMIN privileges to directly dereference a NULL pointer in xfrm_update_ae_params(), leading to a possible kernel crash and denial of service. (CVE-2023-3772)

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://ubuntu.com/security/notices/USN-6465-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0004

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-3772 |
| CVE | CVE-2023-31083 |
| XREF | USN:6465-1 |

## Plugin Information

Published: 2023/10/31, Modified: 2024/01/09

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-88-generic
 for this advisory.
```

## 197214 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6775-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6775-1 advisory.

- The brcm80211 component in the Linux kernel through 6.5.10 has a brcmf_cfg80211_detach use-after-free in the device unplugging (disconnect the USB by hotplug) code. For physically proximate attackers with local access, this could be exploited in a real world scenario. This is related to brcmf_cfg80211_escan_timeout_worker in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c.

(CVE-2023-47233)

- In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix potential key use-after-free When ieee80211_key_link() is called by ieee80211_gtk_rekey_add() but returns 0 due to KRACK protection (identical key reinstall), ieee80211_gtk_rekey_add() will still return a pointer into the key, in a potential use-after-free. This normally doesn't happen since it's only called by iwlwifi in case of WoWLAN rekey offload which has its own KRACK protection, but still better to fix, do that by returning an error code and converting that to success on the cfg80211 boundary only, leaving the error for bad callers of ieee80211_gtk_rekey_add(). (CVE-2023-52530)

- In the Linux kernel, the following vulnerability has been resolved: tomoyo: fix UAF write bug in tomoyo_write_control() Since tomoyo_write_control() updates head->write_buf when write() of long lines is requested, we need to fetch head->write_buf after head->io_sem is held. Otherwise, concurrent write() requests can cause use-after-free-write and double-free problems. (CVE-2024-26622)

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://ubuntu.com/security/notices/USN-6775-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

5.9

EPSS Score

0.0004

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-47233 |
| CVE | CVE-2023-52530 |
| CVE | CVE-2024-26622 |
| XREF | USN:6775-1 |

Plugin Information

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

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-107-
generic for this advisory.
```

## 201864 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6869-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6869-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystem:

- Netfilter; (CVE-2024-26924, CVE-2024-26643)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6869-1

### Solution

Update the affected kernel package.

### Risk Factor

Low

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0004

## CVSS v2.0 Base Score

3.8 (CVSS2#AV:L/AC:H/Au:S/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2024-26643 |
| CVE | CVE-2024-26924 |
| XREF | USN:6869-1 |

## Plugin Information

Published: 2024/07/04, Modified: 2024/07/04

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-113-
generic for this advisory.
```

## 205227 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6950-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6950-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM32 architecture;

- ARM64 architecture;

- Block layer subsystem;

- Bluetooth drivers;

- Clock framework and drivers;

- FireWire subsystem;

- GPU drivers;

- InfiniBand drivers;

- Multiple devices driver;

- EEPROM drivers;

- Network drivers;

- Pin controllers subsystem;

- Remote Processor subsystem;

- S/390 drivers;

- SCSI drivers;

- 9P distributed file system;

- Network file system client;

- SMB network file system;

- Socket messages infrastructure;

- Dynamic debug library;

- Bluetooth subsystem;

- Networking core;

- IPv4 networking;

- IPv6 networking;

- Multipath TCP;

- NSH protocol;

- Phonet protocol;

- TIPC protocol;

- Wireless networking;

- Key management;

- ALSA framework;

- HD-audio driver; (CVE-2024-36883, CVE-2024-36940, CVE-2024-36902, CVE-2024-36975, CVE-2024-36964, CVE-2024-36938, CVE-2024-36931, CVE-2024-35848, CVE-2024-26900, CVE-2024-36967, CVE-2024-36904, CVE-2024-27398, CVE-2024-36031, CVE-2023-52585, CVE-2024-36886, CVE-2024-36937, CVE-2024-36954, CVE-2024-36916, CVE-2024-36905, CVE-2024-36959, CVE-2024-26980, CVE-2024-26936, CVE-2024-36928, CVE-2024-36889, CVE-2024-36929, CVE-2024-36933, CVE-2024-27399, CVE-2024-36946, CVE-2024-36906, CVE-2024-36965, CVE-2024-36957, CVE-2024-36941, CVE-2024-36897, CVE-2024-36952, CVE-2024-36947, CVE-2024-36950, CVE-2024-36880, CVE-2024-36017, CVE-2023-52882, CVE-2024-36969, CVE-2024-38600, CVE-2024-36955, CVE-2024-36960, CVE-2024-27401, CVE-2024-36919, CVE-2024-36934, CVE-2024-35947, CVE-2024-36953, CVE-2024-36944, CVE-2024-36939)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6950-1

## Solution

Update the affected kernel package.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

EPSS Score

0.0005

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-52585 |
| CVE | CVE-2023-52882 |
| CVE | CVE-2024-26900 |
| CVE | CVE-2024-26936 |
| CVE | CVE-2024-26980 |
| CVE | CVE-2024-27398 |
| CVE | CVE-2024-27399 |
| CVE | CVE-2024-27401 |
| CVE | CVE-2024-35848 |
| CVE | CVE-2024-35947 |
| CVE | CVE-2024-36017 |
| CVE | CVE-2024-36031 |
| CVE | CVE-2024-36880 |
| CVE | CVE-2024-36883 |
| CVE | CVE-2024-36886 |
| CVE | CVE-2024-36889 |
| CVE | CVE-2024-36897 |
| CVE | CVE-2024-36902 |
| CVE | CVE-2024-36904 |
| CVE | CVE-2024-36905 |
| CVE | CVE-2024-36906 |
| CVE | CVE-2024-36916 |
| CVE | CVE-2024-36919 |
| CVE | CVE-2024-36928 |
| CVE | CVE-2024-36929 |
| CVE | CVE-2024-36931 |
| CVE | CVE-2024-36933 |
| CVE | CVE-2024-36934 |
| CVE | CVE-2024-36937 |

| | |
|---|---|
| CVE | CVE-2024-36938 |
| CVE | CVE-2024-36939 |
| CVE | CVE-2024-36940 |
| CVE | CVE-2024-36941 |
| CVE | CVE-2024-36944 |
| CVE | CVE-2024-36946 |
| CVE | CVE-2024-36947 |
| CVE | CVE-2024-36950 |
| CVE | CVE-2024-36952 |
| CVE | CVE-2024-36953 |
| CVE | CVE-2024-36954 |
| CVE | CVE-2024-36955 |
| CVE | CVE-2024-36957 |
| CVE | CVE-2024-36959 |
| CVE | CVE-2024-36960 |
| CVE | CVE-2024-36964 |
| CVE | CVE-2024-36965 |
| CVE | CVE-2024-36967 |
| CVE | CVE-2024-36969 |
| CVE | CVE-2024-36975 |
| CVE | CVE-2024-38600 |
| XREF | USN:6950-1 |

## Plugin Information

Published: 2024/08/08, Modified: 2024/08/08

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-87-generic does not meet the minimum fixed level of 5.15.0-118-
generic for this advisory.
```

## 156000 - Apache Log4j Installed (Linux / Unix)

### Synopsis

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

### Description

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

The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' scanner setting in Nessus 8.15.1 or later.

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

### See Also

https://logging.apache.org/log4j/2.x/

### Solution

n/a

### Risk Factor

None

### References

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

### Plugin Information

Published: 2021/12/10, Modified: 2024/08/08

### Plugin Output

tcp/0

```
  Path                           : /usr/share/java/libintl-0.21.jar
  Version                        : unknown
  JMSAppender.class association  : Not Found
  JdbcAppender.class association : Not Found
  JndiLookup.class association   : Not Found
  Method                         : Embedded string inspection


Note: Jar file inspection cannot be performed.  No results or cannot list archive contents.  If
 results are present, install an unzip package to resolve this problem.
```

## 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      : 1.2a
Vendor       : American Megatrends International, LLC.
Release Date : 06/02/2023
UUID         : 8a03b400-a7ae-11ed-8000-3cecefde9ac2
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: 2024/07/31

### Plugin Output

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:22.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:log4j -> Apache Software Foundation log4j
  cpe:/a:docker:docker:26.1.4 -> Docker
  cpe:/a:gnupg:libgcrypt:1.8.8 -> GnuPG Libgcrypt
  cpe:/a:gnupg:libgcrypt:1.9.4 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.81.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.81.0 -> Haxx libcurl
  cpe:/a:openbsd:openssh:8.9 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:8.9p1 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.1.1k -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.1.1n -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.1.1w -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:3.0.2 -> OpenSSL Project OpenSSL
```

```
cpe:/a:openssl:openssl:3.1.3 -> OpenSSL Project OpenSSL
cpe:/a:sqlite:sqlite -> SQLite
cpe:/a:tukaani:xz -> Tukaani XZ
cpe:/a:tukaani:xz:5.2.5 -> Tukaani XZ
cpe:/a:tukaani:xz:5.4.3 -> Tukaani XZ
cpe:/a:vim:vim:8.2 -> 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: 2024/08/08

### Plugin Output

tcp/0

```
Path               : /usr/bin/curl
Version            : 7.81.0
Associated Package : curl 7.81.0-1ubuntu1.16
Managed by OS      : True
```

## 132634 - Deprecated SSLv2 Connection Attempts

### Synopsis

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

### Description

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

### Solution

N/A

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

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

Plugin ID: 42476
Timestamp: 2024-08-12 11:50:22
Port: 22
```

## 55472 - Device Hostname

### Synopsis

It was possible to determine the remote system hostname.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/06/30, Modified: 2024/08/06

### Plugin Output

tcp/0

```
Hostname : s01.chthu1.arma
  s01.chthu1.arma (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 : 100
```

## 111529 - Docker Container Number of Changed Files

### Synopsis

Checks for changes in running Docker containers and reports how many files changed.

### Description

This plugin checks the docker diff information for each container and reports the number of changed files.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/08/03, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Docker container f6ac6812ed3a9437063edbbf607861e3c08d171ac7ab322ce3636879fd5031a8 has 7 changed
 files

Docker container fd953986438de6423f022d2c9a2935e936aee7a29755aa89a1c30827d2e274c4 has 6 changed
 files

Docker container 447c6f740623d46cc5e3578367de8d18ed54282fc5f8d56a0a838fff43233d2d has 5 changed
 files

Docker container 9b4e7286984ac88e000c710b18e895fa7cf263e4fb62a75136364ceb5be05f22 has 26 changed
 files

Docker container 53e18fd814788fb646908f4cf322887b66d58ae4b18d5dd909848e82a4077385 has 6 changed
 files

Docker container 27e6c16338a5aff512b4e387f5a2b2afa477563f43fb73cd416fa8a8f780aad4 has 6 changed
 files

Docker container 035b294c5332421f197d427e2fabdbf063ad8928934561719105 4784a348ee7a has 14 changed
 files

Docker container 33ff736962f3b539a256379ddba10ecad77aff7edc1b96cceb38c1df01451a83 has 18 changed
 files
```

```
Docker container c9b9ed4384ab7404324963ff7ca7efece9edb901caaf57554ce061e82f053865 has 6 changed
 files

Docker container dd6ab659bfdc73e75ce836915d1c59aac420a2b4c8e71f38acb3f7eb7a13b1ee has 9 changed
 files

Docker container 3327201a25fb4c1e760cafcbaf0df974a7ada9148457579b355e7c568a308c2c has 3 changed
 files
```

## 159488 - Docker Installed (Linux)

### Synopsis

Docker was detected on the remote host.

### Description

A container virtualization suite is installed on the remote host.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/04, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Path    : /usr/bin/docker
Version : 26.1.4
build   : 5650f9b
```

## 93561 - Docker Service Detection

### Synopsis

Docker was detected on the remote host.

### Description

The Docker service is running on the remote host. Docker is an open-source project that automates the deployment of applications inside software containers.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/09/16, Modified: 2024/08/08

### Plugin Output

tcp/0

```
  Version: 26.1.4
  Version: 26.1.4
  Version: 1.6.33
  Version: 1.1.12
  Version: 0.19.0

The following containers were detected running on the remote Docker host :

Name:      /dataplane-control
Image:     scion-all
Image ID : sha256:6748551f7a00366f8fc7a1701f791e8e9405eb6ec71fc627b267f6f852eb307c
Tag:       v0.36.2
ID:        f6ac6812ed3a9437063edbbf607861e3c08d171ac7ab322ce3636879fd5031a8
Ports:     n/a

Name:      /promtail
Image:     promtail
Image ID : sha256:f5f9b65df51eaeab920fa0ddb2842993e6141c8f539c765df0539d32d8f40802
Tag:       v0.36.2
ID:        fd953986438de6423f022d2c9a2935e936aee7a29755aa89a1c30827d2e274c4
Ports:     n/a

Name:      /node-exporter
Image:     node-exporter
```

```
Image ID : sha256:635028d8e9e95336a5e6970af6502ecc691302cb105671fc504caed474c443c7
Tag:       v0.36.2
ID:        447c6f740623d46cc5e3578367de8d18ed54282fc5f8d56a0a838fff43233d2d
Ports:     n/a

Name:      /control-64-2_0_2c
Image:     scion-all
Image ID : sha256:6748551f7a00366f8fc7a1701f791e8e9405eb6ec71fc627b267f6f852eb307c
Tag:       v0.36.2
ID:        9b4e7286984ac88e000c710b18e895fa7cf263e4fb62a75136364ceb5be05f22
Ports:     n/a

Name:      /router
Image:     scion-all
Image ID : sha256:6748551f7a00366f8fc7a1701f791e8e9405eb6ec71fc627b267f6f852eb307c
Tag:       v0.36.2
ID:        53e18fd814788fb646908f4cf322887b66d58ae4b18d5dd909848e82a4077385
Ports:     n/a

Name:      /dispatcher
Image:     scion-all
Image ID : sha256:6748551f7a00366f8fc7a1701f791e8e9405eb6ec71fc627b267f6f852eb307c
Tag:       v0.36.2
ID:        27e6c16338a5aff512b4e387f5a2b2afa477563f43fb73cd416fa8a8f780aad4
Ports:     n/a

Name:      /daemon-64-2_0_2c
Image:     scion-all
Image ID : sha256:6748551f7a00366f8fc7a1701f791e8e9405eb6ec71fc627b267f6f852eb307c
Tag:       v0.36.2
ID:        035b294c5332421f197d427e2fabdbf063ad8928934561719105478 4a348ee7a
Ports:     n/a

Name:      /dataplane
Image:     vpp-dataplane
Image ID : sha256:83c13244bfbda00bb6e8b5fa39eeecc8c1b57dd94ed2734c42acbf46e2dc4560
Tag:       v0.36.2
ID:        33ff736962f3b539a256379ddba10 [...]
```

## 25203 - Enumerate IPv4 Interfaces via SSH

### Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

### Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

### Solution

Disable any unused IPv4 interfaces.

### Risk Factor

None

### Plugin Information

Published: 2007/05/11, Modified: 2024/02/05

### Plugin Output

tcp/0

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

 - 172.17.0.1 (on interface docker0)
 - 195.144.33.209 (on interface eno3)
 - 10.20.0.102 (on interface eno4)
 - 192.168.110.1 (on interface eno7)
 - 217.193.19.214 (on interface eno8)
 - 127.0.0.1 (on interface lo)
 - 198.18.30.1 (on interface wg0)
 - 198.19.6.4 (on interface wg1)
```

## 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 :

 - fe80::3eec:efff:fede:9ac4 (on interface eno3)
 - fe80::3eec:efff:fede:9ac5 (on interface eno4)
 - fe80::3eec:efff:fede:9d5e (on interface eno7)
 - fe80::3eec:efff:fede:9d5f (on interface eno8)
 - ::1 (on interface lo)
 - fe80::5989:f329:d605:16bc (on interface scion-gateway)
```

## 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 :

  - 3c:ec:ef:de:9a:c5 (interface eno4)
  - 3c:ec:ef:dd:55:e1 (interface enp22s0f3)
  - 3c:ec:ef:de:9a:c4 (interface eno3)
  - 3c:ec:ef:de:9a:c2 (interface eno1)
  - 3c:ec:ef:de:9d:5f (interface eno8)
  - 3c:ec:ef:dd:55:e0 (interface enp22s0f2)
  - 3c:ec:ef:de:9d:5e (interface eno7)
  - 3c:ec:ef:dd:55:de (interface enp22s0f0)
  - 3c:ec:ef:de:9b:ce (interface eno5)
  - 02:42:1e:55:59:53 (interface docker0)
  - 3c:ec:ef:de:9b:cf (interface eno6)
  - 3c:ec:ef:dd:55:df (interface enp22s0f1)
  - b0:3a:f2:b6:05:9f (interface enxb03af2b6059f)
```

## 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

```
enxb03af2b6059f:
  MAC : b0:3a:f2:b6:05:9f
eno8:
  MAC : 3c:ec:ef:de:9d:5f
  IPv4:
    - Address : 217.193.19.214
      Netmask : 255.255.255.252
      Broadcast : 217.193.19.215
  IPv6:
    - Address : fe80::3eec:efff:fede:9d5f
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
enp22s0f1:
  MAC : 3c:ec:ef:dd:55:df
eno6:
  MAC : 3c:ec:ef:de:9b:cf
eno7:
  MAC : 3c:ec:ef:de:9d:5e
  IPv4:
    - Address : 192.168.110.1
      Netmask : 255.255.255.0
      Broadcast : 192.168.110.255
  IPv6:
    - Address : fe80::3eec:efff:fede:9d5e
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
wg1:
  IPv4:
    - Address : 198.19.6.4
      Netmask : 255.255.255.255
```

```
eno1:
  MAC : 3c:ec:ef:de:9a:c2
enp22s0f0:
  MAC : 3c:ec:ef:dd:55:de
eno4:
  MAC : 3c:ec:ef:de:9a:c5
  IPv4:
    - Address : 10.20.0.102
        Netmask : 255.255.0.0
        Broadcast : 10.20.255.255
  IPv6:
    - Address : fe80::3eec:efff:fede:9ac5
        Prefixlen : 64
        Scope : link
        ScopeID : 0x20
enp22s0f3:
  MAC : 3c:ec:ef:dd:55:e1
eno3:
  MAC : 3c:ec:ef:de:9a:c4
  IPv4:
    - Address : 195.144.33.209
        Netmask : 255.255.255.248
        Broadcast : 195.144.33.215
  IPv6:
    - Address : fe80::3eec:efff:fede:9ac4
        Prefixlen : 64
        Scope : link
        ScopeID : 0x20
wg0:
  IPv4:
    - Address : 198.18.30.1
        Netmask : 255.255.255.255
scion-gateway:
  IPv6:
    - Address : fe80::5989:f329:d605:16bc
        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
enp22s0f2:
  MAC : 3c:ec:ef:dd:55:e0
eno5:
  MAC : 3c:ec:ef:de:9b:ce
docker0:
  MAC : 02:42:1e:55:59:53
  IPv4:
    - Address : 172.17.0.1
        Netmask : 255.255.0.0
        Broadcast : 172.17.255.255
```

## 179200 - Enumerate the Network Routing configuration via SSH

### Synopsis

Nessus was able to retrieve network routing information from the remote host.

### Description

Nessus was able to retrieve network routing information the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/08/02, Modified: 2023/08/02

### Plugin Output

tcp/0

```
Gateway Routes:
  eno7:
    ipv4_gateways:
      192.168.110.2:
        subnets:
          - 0.0.0.0/0
  eno8:
    ipv4_gateways:
      217.193.19.213:
        subnets:
          - 193.247.168.0/21
          - 195.65.89.0/25
  wg0:
    ipv4_gateways:
      198.18.0.1:
        subnets:
          - 198.18.0.0/24
Interface Routes:
  docker0:
    ipv4_subnets:
      - 172.17.0.0/16
  eno3:
    ipv4_subnets:
      - 195.144.33.208/29
    ipv6_subnets:
      - fe80::/64
  eno4:
    ipv4_subnets:
      - 10.20.0.0/16
    ipv6_subnets:
      - fe80::/64
  eno7:
```

```
    ipv4_subnets:
     - 192.168.110.0/24
    ipv6_subnets:
     - fe80::/64
  eno8:
    ipv4_subnets:
     - 217.193.19.212/30
    ipv6_subnets:
     - fe80::/64
  scion-gateway:
    ipv4_subnets:
     - 31.10.128.0/18
     - 31.10.128.0/17
     - 31.10.192.0/18
     - 31.10.193.192/30
     - 31.10.249.240/29
     - 31.164.0.0/16
     - 31.164.0.0/15
     - 31.165.0.0/16
     - 31.222.24.0/24
     - 31.222.30.0/24
     - 45.10.168.0/22
     - 45.85.99.0/24
     - 45.143.156.0/24
     - 46.14.0.0/16
     - 46.126.0.0/16
     - 46.126.0.0/15
     - 46.127.0.0/16
     - 46.140.0.0/17
     - 46.140.0.0/16
     - 46.140.128.0/17
     - 46.140.182.240/29
     - 62.2.0.0/17
     - 62.2.0.0/16
     - 62.2.128.0/17
     - 62.167.0.0/17
     - 62.167.0.0/16
     - 62.167.128.0/17
     - 62.192.17.0/24
     - 62.202.0.0/16
     - 62.203.0.0/16
     - 62.240.192.0/19
     - 77.56.0.0/15
     - 77.56.0.0/14
     - 77.58.0.0/15
     - 77.72.64.0/21
     - 77.111.232.0/22
     - 80.67.144.0/20
     - 80.94.144.0/20
     - 80.218.0.0/16
     - 80.218.0.0/15
     - 80.219.0.0/16
     - 81.7.224.0/20
     - 81.7.224.0/19
     - 81.7.240.0/20
     - 81.62.0.0/15
     - 83.76.0.0/15
     - 83.78.0.0/15
     - 83.137.72.0/21
     - 83.173.192.0/18
     - 84.20.32.0/21
     - 84.20.32.0/20
     - 84.20.40.0/21
     - 84.20.48.0/22
     - 84.20.48.0/21
     - 84.20.52.0/22
     - 84.72.0.0/15
     - 84.72.0.0/14
     - 84.74.0.0/15
     - 84.226.0.0/16
```

```
      - 84.226.0.0/15
      - 84.227.0.0/16
   [...]
```

## 168980 - Enumerate the PATH Variables

### Synopsis

Enumerates the PATH variable of the current scan user.

### Description

Enumerates the PATH variables of the current scan user.

### Solution

Ensure that directories listed here are in line with corporate policy.

### Risk Factor

None

### Plugin Information

Published: 2022/12/21, Modified: 2024/08/08

### 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
/snap/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 :

3C:EC:EF:DE:9D:5E : Super Micro Computer, Inc.
3C:EC:EF:DE:9A:C5 : Super Micro Computer, Inc.
3C:EC:EF:DD:55:E1 : Super Micro Computer, Inc.
3C:EC:EF:DE:9A:C4 : Super Micro Computer, Inc.
3C:EC:EF:DE:9A:C2 : Super Micro Computer, Inc.
3C:EC:EF:DE:9D:5F : Super Micro Computer, Inc.
3C:EC:EF:DD:55:E0 : Super Micro Computer, Inc.
3C:EC:EF:DD:55:DE : Super Micro Computer, Inc.
3C:EC:EF:DE:9B:CE : Super Micro Computer, Inc.
3C:EC:EF:DE:9B:CF : Super Micro Computer, Inc.
3C:EC:EF:DD:55:DF : Super Micro Computer, Inc.
```

## 86420 - Ethernet MAC Addresses

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 3C:EC:EF:DE:9D:5E
  - 3C:EC:EF:DE:9A:C5
  - 3C:EC:EF:DD:55:E1
  - 3C:EC:EF:DE:9A:C4
  - 3C:EC:EF:DE:9A:C2
  - 3C:EC:EF:DE:9D:5F
  - 3C:EC:EF:DD:55:E0
  - 3C:EC:EF:DD:55:DE
  - 3C:EC:EF:DE:9B:CE
  - 02:42:1E:55:59:53
  - 3C:EC:EF:DE:9B:CF
  - 3C:EC:EF:DD:55:DF
  - B0:3A:F2:B6:05:9F
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/443/www

```
1 external URL was gathered on this web server :
URL...                                  - Seen on...


https://fonts.gstatic.com               - /ui
```

## 84502 - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

https://tools.ietf.org/html/rfc6797

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
HTTP/1.1 301 Moved Permanently
Alt-Svc: h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000
Content-Length: 38
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Aug 2024 11:50:49 GMT
Location: /ui
Server: Caddy
Connection: close

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

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Based on tests of each method :

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

    /
    /ui
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

```
Based on tests of each method :

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

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The remote web server type is :

Caddy
```

## 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/42001/www

```
The remote web server type is :

Caddy
```

## 85805 - HTTP/2 Cleartext Detection

### Synopsis

An HTTP/2 server is listening on the remote host.

### Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

### See Also

https://http2.github.io/

https://tools.ietf.org/html/rfc7540

https://github.com/http2/http2-spec

### Solution

Limit incoming traffic to this port if desired.

### Risk Factor

None

### Plugin Information

Published: 2015/09/04, Modified: 2022/04/11

### Plugin Output

tcp/30252

```
The server supports direct HTTP/2 connections
without encryption.
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 301 Moved Permanently

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

  Alt-Svc: h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000
  Content-Length: 38
  Content-Type: text/html; charset=utf-8
  Date: Mon, 12 Aug 2024 11:51:07 GMT
  Location: /ui
  Server: Caddy
  Connection: close

Response Body :

<a href="/ui">Moved Permanently</a>.
```

## 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/42001/www

```
Response Code : HTTP/1.1 200 OK

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

  Server: Caddy
  Date: Mon, 12 Aug 2024 11:51:07 GMT
  Content-Length: 0
  Connection: close

Response Body :
```

## 91634 - HyperText Transfer Protocol (HTTP) Redirect Information

### Synopsis

The remote web server redirects requests to the root directory.

### Description

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

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

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Request         : https://192.168.110.1/
HTTP response   : HTTP/1.1 301 Moved Permanently
Redirect to     : https://192.168.110.1/ui
Redirect type   : 30x redirect

Final page      : https://192.168.110.1/ui
HTTP response   : HTTP/1.1 200 OK
```

## 171410 - IP Assignment Method Detection

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/02/14, Modified: 2024/08/08

### Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ eno1
+ enxb03af2b6059f
+ enp22s0f0
+ eno4
  + IPv4
    - Address       : 10.20.0.102
      Assign Method : static
  + IPv6
    - Address       : fe80::3eec:efff:fede:9ac5
      Assign Method : static
+ enp22s0f1
+ eno5
+ enp22s0f2
+ enp22s0f3
+ eno6
+ wg0
  + IPv4
    - Address       : 198.18.30.1
      Assign Method : static
+ wg1
  + IPv4
    - Address       : 198.19.6.4
      Assign Method : static
+ docker0
  + IPv4
```

```
    - Address       : 172.17.0.1
      Assign Method : static
+ eno3
  + IPv4
    - Address       : 195.144.33.209
      Assign Method : static
  + IPv6
    - Address       : fe80::3eec:efff:fede:9ac4
      Assign Method : static
+ eno7
  + IPv4
    - Address       : 192.168.110.1
      Assign Method : static
  + IPv6
    - Address       : fe80::3eec:efff:fede:9d5e
      Assign Method : static
+ eno8
  + IPv4
    - Address       : 217.193.19.214
      Assign Method : static
  + IPv6
    - Address       : fe80::3eec:efff:fede:9d5f
      Assign Method : static
+ i.ABAAAAQAAAACY
+ scion-gateway
  + IPv6
    - Address       : fe80::5989:f329:d605:16bc
      Assign Method : static
```

## 118237 - JAR File Detection for Linux/UNIX

### Synopsis

Detected JAR files on the host.

### Description

The host contains JAR files, Java Archive files.

Note that this plugin only detects JAR files in commonly used installation directories or a user specified search path.

### See Also

https://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/22, Modified: 2024/08/08

### Plugin Output

tcp/0

```
JAR files found: 1
 - /usr/share/java/libintl-0.21.jar
```

## 151883 - Libgcrypt Installed (Linux/UNIX)

### Synopsis

Libgcrypt is installed on this host.

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/07/21, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 50 installs of Libgcrypt:

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /run/initramfs/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /run/initramfs/lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /run/initramfs/usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /run/initramfs/usr/lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /var/run/initramfs/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /var/run/initramfs/lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
```

```
  Version : 1.9.4

  Path    : /var/run/initramfs/usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /var/run/initramfs/usr/lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/var/run/initramfs/
lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/var/run/initramfs/
lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/var/run/initramfs/
usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/var/run/initramfs/
usr/lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/XXNL2YYIEL57MDEJQ55GJDCA5Q/var/run [...]
```

## 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
tmpfs                              3.1G   22M  3.1G   1% /run
/dev/mapper/vg--main-lv--root      219G   14G  195G   7% /
tmpfs                               16G     0   16G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          406M  216M  158M  58% /boot
/dev/mapper/vg--secondary-lv--var  219G  9.9G  198G   5% /var
/dev/sda1                          127M  6.1M  120M   5% /boot/efi
overlay                            219G  9.9G  198G   5% /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged
overlay                            219G  9.9G  198G   5% /var/lib/docker/
overlay2/3b07aa344b00e4433128bd71ffe6a6427e4aefc5b23d5000d67257857cf05e39/merged
overlay                            219G  9.9G  198G   5% /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged
overlay                            219G  9.9G  198G   5% /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged
overlay                            219G  9.9G  198G   5% /var/lib/docker/overlay2/
e25779e9ec768b48cdac6986bd8c72aa3cb1d38f530dc5f971831d242312f09d/merged
overlay                            219G  9.9G  198G   5% /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged
overlay                            219G  9.9G  198G   5% /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged
overlay                            219G  9.9G  198G   5% /var/lib/docker/
overlay2/39c7d30c5a5b728cf2e790aaa8217b958882a1059cf94f47ffef44fc62756611/merged
```

```
overlay                          219G  9.9G  198G   5% /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged
overlay                          219G  9.9G  198G   5% /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c679 [...]
```

## 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: Etc/UTC (UTC, +0000)
Via /etc/timezone: Etc/UTC
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: 2024/03/13

### Plugin Output

tcp/0

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

User         : anapaya
Home folder  : /home/anapaya
Start script : /bin/bash
Groups       : users
               docker
               admin

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

User         : root
Home folder  : /root
Start script : /bin/bash
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  : /run/ircd
Start script : /usr/sbin/nologin
Groups       : irc

User         : gnats
Home folder  : /var/lib/gnats
Start script : /usr/sbin/nologin
Groups       : gnats

User         : nobody
Home folder  : /nonexistent
Start script : /usr/sbin/nologin
```

```
Groups       : nogroup

User         : _apt
Home folder [...]
```

## 45433 - Memory Information (via DMI)

### Synopsis

Information about the remote system's memory devices can be read.

### Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/06, Modified: 2018/03/29

### Plugin Output

tcp/0

```
Total memory : 32768 MB
```

## 50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

### See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

### Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/443/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - https://192.168.110.1/ui
  - https://192.168.110.1/ui/
```

## 50345 - Missing or Permissive X-Frame-Options HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

### See Also

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

http://www.nessus.org/u?399b1f56

### Solution

Set a properly configured X-Frame-Options header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/443/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - https://192.168.110.1/ui
  - https://192.168.110.1/ui/
```

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/08/05

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.1
Nessus build : 20004
Plugin feed version : 202408120709
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Advanced Scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.110.80
Port scanner(s) : netstat
Port range : 0-65535
Ping RTT : 217.125 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'anapaya' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : never
Max hosts : 100
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 : 2024/8/12 13:48 CEST
Scan duration : 1183 sec
Scan for malware : yes
```

## 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: 2024/07/31

### Plugin Output

tcp/0

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

193.247.172.2 connected to port 42001 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: 2024/07/24

### 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: 2024/07/24

### Plugin Output

tcp/443/www

```
Port 443/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: 2024/07/24

### Plugin Output

udp/443

```
Port 443/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: 2024/07/24

### Plugin Output

udp/30041

```
Port 30041/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: 2024/07/24

### Plugin Output

udp/30042

```
Port 30042/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: 2024/07/24

### Plugin Output

tcp/30252

```
Port 30252/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: 2024/07/24

### Plugin Output

tcp/42001/www

```
Port 42001/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: 2024/07/24

### Plugin Output

udp/51021

```
Port 51021/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: 2024/07/24

### Plugin Output

udp/51022

```
Port 51022/udp was found to be open
```

## 33851 - Network daemons not managed by the package system

### Synopsis

Some daemon processes on the remote host are associated with programs that have been installed manually.

### Description

Some daemon processes on the remote host are associated with programs that have been installed manually.

System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

### Solution

Use packages supplied by the operating system vendor whenever possible.

And make sure that manual software installation agrees with your organization's acceptable use and security policies.

### Risk Factor

None

### Plugin Information

Published: 2008/08/08, Modified: 2024/03/06

### Plugin Output

tcp/0

```
The following running daemons are not managed by dpkg :

/usr/local/bin/appliance
/usr/local/bin/debugscraper
```

## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/12/09, Modified: 2024/06/19

### Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 5.15.0-87-generic on Ubuntu 22.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 5.15.0-87-generic on Ubuntu 22.04
```

## 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: 2024/03/19

### Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'publickey' authentication.

The output of "uname -a" is :
Linux s01.chthu1.arma 5.15.0-87-generic #97-Ubuntu SMP Mon Oct 2 21:09:21 UTC 2023 x86_64 x86_64
 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
bookworm/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 28.183314 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.

Account  : anapaya
Protocol : SSH
```

## 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: 2024/08/08

### Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.9p1
Banner  : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
```

## 168007 - OpenSSL Installed (Linux)

### Synopsis

OpenSSL was detected on the remote Linux host.

### Description

OpenSSL was detected on the remote Linux host.

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

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

### See Also

https://openssl.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/11/21, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 43 installs of OpenSSL:

  Path    : /var/lib/docker/overlay2/
b58f61c66b3ce0d46dc469e103e231252fd95fce68898af577744c7de9f90924/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.3
  Version : 3.0.2

  Path    : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Version : 1.1.1k
```

```
  Path    : /var/lib/docker/overlay2/
a9e2a4c0e6b55bfef864826ed0fba96de2f20dd9b5d3ed31e123782be960caf6/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/13102d56596f7e6d24798cfe891504e6325ee229c23659e039f687efed21e583/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/9218100d278bb813c373ccb4bd2e5a6d6dba7c8ecd4b73682f35380c67947208/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/62a912c96ae172daa0e09bba120b0e85a45449881a13653c1b37e9f0e4beeeda/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
f59753112224f4c06036be05e3d15a4c010784b2c980c952cd38823a3616becb/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
e749a9a2418355564c3a2c0b690663d1684d4a12c9976451ae742e4430121c43/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/5c5ec55dc2d7b2a92e2540bfd039911b23b96d952cc851f6b3ab164950412a15/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Version : 1.1.1n

  Path    : /var/lib/docker/overlay2/3b07aa344b00e4433128bd71ffe6a6427e4ae [...]
```

## 66334 - Patch Report

### Synopsis

The remote host is missing several patches.

### Description

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

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

### Solution

Install the patches listed below.

### Risk Factor

None

### Plugin Information

Published: 2013/07/08, Modified: 2024/07/15

### Plugin Output

tcp/0

```
. You need to take the following 33 actions :

[ Docker Engine < 23.0.15 / 26.x < 26.1.5 / 27.x < 27.1.1 Authentication Bypass (204784) ]

+ Action to take : Upgrade to Docker Engine version 23.0.15, 26.1.5, 27.1.1 or later

[ OpenSSL 1.1.1 < 1.1.1za Vulnerability (201084) ]

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

[ OpenSSL 3.0.0 < 3.0.15 Vulnerability (201085) ]

+ Action to take : Upgrade to OpenSSL version 3.0.15 or later.

+Impact : Taking this action will resolve 40 different vulnerabilities (CVEs).


[ OpenSSL 3.1.0 < 3.1.7 Vulnerability (201082) ]

+ Action to take : Upgrade to OpenSSL version 3.1.7 or later.
```

```
[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Python vulnerabilities
 (USN-6891-1) (202187) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 41 different vulnerabilities (CVEs).


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability
 (USN-6640-1) (190598) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos
 vulnerabilities (USN-6947-1) (205195) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)
 (185568) ]

+ Action to take : Update the affected traceroute package.


[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1) (195216) ]

+ Action to take : Update the affected packages.


[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : NSS vulnerabilities (USN-6727-1) (193171) ]

+ Action to take : Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Bind vulnerabilities (USN-6909-1) (203144) ]

+ Action to take : Update the  [...]
```

## 45432 - Processor Information (via DMI)

### Synopsis

Nessus was able to read information about the remote system's processor.

### Description

Nessus was able to retrieve information about the remote system's hardware, such as its processor type, by using the SMBIOS (aka DMI) interface.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/06, Modified: 2016/02/25

### Plugin Output

tcp/0

```
Nessus detected 1 processor :

Current Speed   : 2100 MHz
Version         : Intel(R) Xeon(R) D-2733NT CPU @ 2.10GHz
Manufacturer    : NO DIMM
External Clock  : 100 MHz
Status          : Populated, Enabled
Family          : Pentium 4
Type            : Unknown
```

## 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   : 2075504
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

tcp/80

```
Process ID   : 2003069
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 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/443/www

```
Process ID   : 2003069
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 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/30041

```
Process ID   : 2075830
Executable   : /app/scion-all
Command line : /app/scion-all dispatcher --config /share/conf/dispatcher.toml
```

## 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/30042

```
Process ID   : 2075848
Executable   : /usr/bin/vpp
Command line : /usr/bin/vpp -c /share/conf/dataplane.conf
```

## 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/30252

```
Process ID   : 2075867
Executable   : /app/scion-all
Command line : /app/scion-all control --config /share/conf/control.toml
```

## 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/42001/www

```
Process ID   : 2003069
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 174788 - SQLite Local Detection (Linux)

### Synopsis

The remote Linux host has SQLite Database software installed.

### Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

### See Also

https://www.sqlite.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/04/26, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Path    : /usr/share/bash-completion/completions/sqlite3
Version : unknown
```

## 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: 2017/08/28

### Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

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

The server supports the following options for server_host_key_algorithms :

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

The server supports the following options for encryption_algorithms_client_to_server :

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

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

The server supports the following options for encryption_algorithms_server_to_client :

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

The server supports the following options for mac_algorithms_client_to_server :

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

The server supports the following options for mac_algorithms_server_to_client :

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

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@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
```

## 90707 - SSH SCP Protocol Detection

### Synopsis

The remote host supports the SCP protocol over SSH.

### Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

### Plugin Output

tcp/22/ssh

## 153588 - SSH SHA-1 HMAC Algorithms Enabled

### Synopsis

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

### Description

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

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/22/ssh

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

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

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

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

## 10267 - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0933

### Plugin Information

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

### Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
SSH supported authentication : publickey
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

### Plugin Output

tcp/443/www

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

## 83298 - SSL Certificate Chain Contains Certificates Expiring Soon

### Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

### Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

### Solution

Renew any soon to expire SSL certificates.

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

|-Subject   : CN=Caddy Local Authority - ECC Intermediate
|-Not After : Aug 16 07:41:24 2024 GMT

|-Subject   :
|-Not After : Aug 12 23:19:12 2024 GMT
```

## 42981 - SSL Certificate Expiry - Future Expiry

### Synopsis

The SSL certificate associated with the remote service will expire soon.

### Description

The SSL certificate associated with the remote service will expire soon.

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The SSL certificate will expire within 60 days, at
Aug 12 23:19:12 2024 GMT :

  Subject          : n/a
  Issuer           : CN=Caddy Local Authority - ECC Intermediate
  Not valid before : Aug 12 11:19:12 2024 GMT
  Not valid after  : Aug 12 23:19:12 2024 GMT
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 00 FE 80 B3 DC 81 7E 47 25 DE 9C 73 53 87 E0 42 62

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:19:12 2024 GMT
Not Valid After: Aug 12 23:19:12 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 49 14 87 98 D1 80 83 7D 87 B4 B3 58 22 39 8F EA 10 9F 66 BE
              EB FF 22 6D D8 0C 30 A4 75 91 58 C1
Public Key Y: C5 49 C1 4B 49 32 3B 15 08 E7 50 CD 9B A2 34 4A B4 5A 7A 16
              0B 51 59 E1 7F 68 BE 7C E8 EA 4D 51

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 E6 A0 44 38 5C 02 0F 08 B3 17 79 A2 CC 8B
           90 5A CC 72 38 57 79 E4 62 1C 79 3C 55 55 A8 10 8F 6B 02 20
           17 BA 06 B2 B3 C3 40 EC 29 84 49 81 C4 0F 49 D9 CF 1F 46 77
           98 10 88 6B 54 F5 3F 2D 30 7D CF 93
```

```
Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CA CE 66 21 AC 7E 00 1D 67 E1 A5 58 9F D0 49 FA C6 17 7A 9F


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 06 FD 5B E3 42 84 BD CB 79 EE 8D D2 22 8E 53 7E 32 DB 27 A9


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1


Fingerprints :

SHA-256 Fingerprint: D0 25 1A 1A 8C A1 05 68 36 EB 20 32 03 E5 77 54 8B F9 BD 75
                     AA F6 2C EF 2A 4A FB 41 B4 5D 8D 1A
SHA-1 Fingerprint: C6 C7 3A D0 4E 50 C8 4B 7F 6A FE 40 52 3C 5C D3 36 56 51 13
MD5 Fingerprint: 46 B4 FE A4 7F 21 9E AD 85 83 51 DE E8 B3 90 04


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV
+gAwIBAgIRAP6As9yBfkcl3pxzU4fgQmIwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVk
 [...]
```

## 159544 - SSL Certificate with no Common Name

### Synopsis

Checks for an SSL certificate with no Common Name

### Description

The remote system is providing an SSL/TLS certificate without a subject common name field. While this is not required in all cases, it is recommended to ensure broad compatibility.

### See Also

https://datatracker.ietf.org/doc/html/rfc5280#section-4.1.2.6

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/06, Modified: 2022/11/30

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 00 FE 80 B3 DC 81 7E 47 25 DE 9C 73 53 87 E0 42 62

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:19:12 2024 GMT
Not Valid After: Aug 12 23:19:12 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 49 14 87 98 D1 80 83 7D 87 B4 B3 58 22 39 8F EA 10 9F 66 BE
              EB FF 22 6D D8 0C 30 A4 75 91 58 C1
Public Key Y: C5 49 C1 4B 49 32 3B 15 08 E7 50 CD 9B A2 34 4A B4 5A 7A 16
```

```
               0B 51 59 E1 7F 68 BE 7C E8 EA 4D 51

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 E6 A0 44 38 5C 02 0F 08 B3 17 79 A2 CC 8B
           90 5A CC 72 38 57 79 E4 62 1C 79 3C 55 55 A8 10 8F 6B 02 20
           17 BA 06 B2 B3 C3 40 EC 29 84 49 81 C4 0F 49 D9 CF 1F 46 77
           98 10 88 6B 54 F5 3F 2D 30 7D CF 93

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CA CE 66 21 AC 7E 00 1D 67 E1 A5 58 9F D0 49 FA C6 17 7A 9F


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 06 FD 5B E3 42 84 BD CB 79 EE 8D D2 22 8E 53 7E 32 DB 27 A9


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV
+gAwIBAgIRAP6As9yBfkcl3pxzU4fgQmIwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVk
qEJ9mvuv/Im3YDDCkdZFYwcVJwUtJMjsVCOdQzZuiNEq0WnoWC1FZ4X9ovnzo6k1Ro4GGMIGDMA4GA1UdDwEB/
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFMrOZiGsfgAdZ+GlWJ/
QSfrGF3qfMB8GA1UdIwQYMBaAFAb9W+NChL3Lee6N0iKOU34y2yepMBIGA1UdEQEB/wQIMAaH [...]
```

## 159545 - SSL Certificate with no Subject

### Synopsis

Checks for an SSL certificate with no Subject

### Description

The remote system is providing an SSL/TLS certificate without a subject field. While this is not required in all cases, it is recommended to ensure broad compatibility.

### See Also

https://datatracker.ietf.org/doc/html/rfc5280#section-4.1.2.6

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/06, Modified: 2022/11/30

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 00 FE 80 B3 DC 81 7E 47 25 DE 9C 73 53 87 E0 42 62

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:19:12 2024 GMT
Not Valid After: Aug 12 23:19:12 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 49 14 87 98 D1 80 83 7D 87 B4 B3 58 22 39 8F EA 10 9F 66 BE
              EB FF 22 6D D8 0C 30 A4 75 91 58 C1
Public Key Y: C5 49 C1 4B 49 32 3B 15 08 E7 50 CD 9B A2 34 4A B4 5A 7A 16
```

```
              0B 51 59 E1 7F 68 BE 7C E8 EA 4D 51

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 E6 A0 44 38 5C 02 0F 08 B3 17 79 A2 CC 8B
           90 5A CC 72 38 57 79 E4 62 1C 79 3C 55 55 A8 10 8F 6B 02 20
           17 BA 06 B2 B3 C3 40 EC 29 84 49 81 C4 0F 49 D9 CF 1F 46 77
           98 10 88 6B 54 F5 3F 2D 30 7D CF 93

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CA CE 66 21 AC 7E 00 1D 67 E1 A5 58 9F D0 49 FA C6 17 7A 9F


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 06 FD 5B E3 42 84 BD CB 79 EE 8D D2 22 8E 53 7E 32 DB 27 A9


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV
+gAwIBAgIRAP6As9yBfkcl3pxzU4fgQmIwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVk
qEJ9mvuv/Im3YDDCkdZFYwcVJwUtJMjsVCOdQzZuiNEq0WnoWC1FZ4X9ovnzo6k1Ro4GGMIGDMA4GA1UdDwEB/
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFMrOZiGsfgAdZ+GlWJ/
QSfrGF3qfMB8GA1UdIwQYMBaAFAb9W+NChL3Lee6N0iKOU34y2yepMBIGA1UdEQEB/wQIMAaH [...]
```

## 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/443/www

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

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


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B        ECDH          ECDSA    AES-GCM(128)
 SHA256
```

```
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C       ECDH           ECDSA    AES-GCM(256)
 SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9       ECDH           ECDSA    ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

## 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

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

### Description

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

### See Also

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

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B        ECDH          ECDSA    AES-GCM(128)
 SHA256
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C        ECDH          ECDSA    AES-GCM(256)
 SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9        ECDH          ECDSA    ChaCha20-Poly1305(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/22/ssh

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

tcp/443/www

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

```
A web server is 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: 2022/09/06

### Plugin Output

tcp/0

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

  ii   adduser  3.118ubuntu5  all  add and remove users and groups
  ii   amd64-microcode  3.20191218.1ubuntu2.2  amd64  Processor microcode firmware for AMD CPUs
  ii   anapaya-appliance-installer  1.2.2  amd64  The installer of the Anapaya appliance.
  ii   anapaya-system-config  1.3.0  amd64  System configuration for Anapaya appliances.
  ii   apparmor  3.0.4-2ubuntu2.3  amd64  user-space parser utility for AppArmor
  ii   apt  2.4.12  amd64  commandline package manager
  ii   apt-transport-https  2.4.12  all  transitional package for https support
  ii   apt-utils  2.4.12  amd64  package management related utility programs
  ii   base-files  12ubuntu4.6  amd64  Debian base system miscellaneous files
  ii   base-passwd  3.5.52build1  amd64  Debian base system master password and group files
  ii   bash  5.1-6ubuntu1.1  amd64  GNU Bourne Again SHell
  ii   bash-completion  1:2.11-5ubuntu1  all  programmable completion for the bash shell
  ii   bind9-dnsutils  1:9.18.24-0ubuntu0.22.04.1  amd64  Clients provided with BIND 9
  ii   bind9-host  1:9.18.24-0ubuntu0.22.04.1  amd64  DNS Lookup Utility
  ii   bind9-libs  1:9.18.24-0ubuntu0.22.04.1  amd64  Shared Libraries used by BIND 9
  ii   binutils  2.38-4ubuntu2.6  amd64  GNU assembler, linker and binary utilities
  ii   binutils-common  2.38-4ubuntu2.6  amd64  Common files for the GNU assembler, linker and
 binary utilities
  ii   binutils-x86-64-linux-gnu  2.38-4ubuntu2.6  amd64  GNU binary utilities, for x86-64-linux-gnu
 target
```

```
ii  bsdextrautils  2.37.2-4ubuntu3.4  amd64  extra utilities from 4.4BSD-Lite
ii  bsdutils  1:2.37.2-4ubuntu3.4  amd64  basic utilities from 4.4BSD-Lite
ii  busybox-initramfs  1:1.30.1-7ubuntu3  amd64  Standalone shell setup for initramfs
ii  bzip2  1.0.8-5build1  amd64  high-quality block-sorting file compressor - utilities
ii  ca-certificates  20230311ubuntu0.22.04.1  all  Common CA certificates
ii  caddy  2.7.5~anapaya3  amd64  Caddy - Powerfu [...]
```

## 118225 - Super Micro detection (dmidecode)

### Synopsis

The remote host is a Super Micro system.

### Description

According to the DMI information, the remote host contains hardware manufactured by Super Micro.

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/19, Modified: 2024/08/08

### Plugin Output

tcp/0

## 35351 - System Information Enumeration (via DMI)

### Synopsis

Information about the remote system's hardware can be read.

### Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/01/12, Modified: 2024/07/29

### Plugin Output

tcp/0

```
Chassis Information
  Serial Number : C515MKL08A30176
  Version       : 0123456789
  Manufacturer  : Supermicro
  Lock          : Not Present
  Type          : Other

System Information
  Serial Number : A500833X3824820
  Version       : 0123456789
  Manufacturer  : Supermicro
  Product Name  : SYS-110D-8C-FRAN8TP
  Family        : Family
```

## 163103 - System Restart Required

### Synopsis

The remote system has updates installed which require a reboot.

### Description

Using the supplied credentials, Nessus was able to determine that the remote system has updates applied that require a reboot to take effect. Nessus has determined that the system has not been rebooted since these updates have been applied, and thus should be rebooted.

### See Also

http://www.nessus.org/u?9e9ce1c1

http://www.nessus.org/u?fd8caec2

### Solution

Restart the target system to ensure the updates are applied.

### Risk Factor

None

### Plugin Information

Published: 2022/07/14, Modified: 2023/11/27

### Plugin Output

tcp/0

```
The following security patches require a reboot but have been installed since the most recent system
 boot:

The reboot required flag is present in the host.

The following packages require a reboot :

systemd
linux-image-5.15.0-112-generic
```

## 25220 - TCP/IP Timestamps Supported

### Synopsis

The remote service implements TCP timestamps.

### Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### See Also

http://www.ietf.org/rfc/rfc1323.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

## 136318 - TLS Version 1.2 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.2.

### See Also

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

### Solution

N/A

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

## 138330 - TLS Version 1.3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.3.

### See Also

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

### Solution

N/A

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

## 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/22/ssh

```
Nessus was able to log into the remote host with no privilege or access
problems via the following :

User:       'anapaya'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo
```

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

### Synopsis

Valid credentials were provided for an available authentication protocol.

### Description

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

Please note the following :

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/22/ssh

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

User:       'anapaya'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo
```

## 56468 - Time of Last System Startup

### Synopsis

The system has been started.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

```
The host has not yet been rebooted.
```

## 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 192.168.110.80 to 192.168.110.1 :
192.168.110.80
192.168.110.1

Hop Count: 1
```

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/03/29, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 10 installs of XZ Utils:

  Path           : /var/lib/docker/
overlay2/635d0259d78b3060578baae6da15db6db7ca992fa93629ef17e95455c3b2eb74/merged/lib/x86_64-linux-
gnu/liblzma.so.5.2.5
  Version        : 5.2.5
```

```
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/overlay2/
e8693cd3cd63d69bffd7b9caf93a582ed7a1102ed145f20c6914486dce89d2ac/diff/usr/lib/liblzma.so.5.4.3
  Version        : 5.4.3
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path    : /var/lib/docker/
overlay2/39c7d30c5a5b728cf2e790aaa8217b958882a1059cf94f47ffef44fc62756611/merged/bin/xz
  Version : unknown

  Path           : /var/lib/docker/
overlay2/9301272284e963a05827d23b732de2f67356a9ba0df6817f69ff9d374c6bf502/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path    : /var/lib/docker/
overlay2/9a878268978351201c872afe94e274fccc90a63b65d2d24e26a3f128738873e4/diff/bin/xz
  Version : unknown

  Path               : /usr/bin/xz
  Version            : 5.2.5
  Associated Package : xz-utils 5.2.5-2ubuntu1
  Confidence         : High
  Managed by OS      : True
  Version Source     : Package

  Path           : /run/initramfs/usr/lib/x86_64-linux-gnu/liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path    : /var/lib/docker/
overlay2/757fc5ca85942486806141d9dd20630b760c0d08fdcb82bf6bc7a5f9961056ef/diff/bin/xz
  Version : unknown

  Path               : /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.5
  Version            : 5.2.5
  Associated Package : liblzma5 5.2.5-2ubuntu1
  Confidence         : High
  Managed by OS      : True
  Version Source     : Package
```

## 193233 - Ubuntu 20.04 LTS / 22.04 LTS : NSS regression (USN-6727-2)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6727-2 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-6727-2

### Solution

Update the affected libnss3, libnss3-dev and / or libnss3-tools packages.

### Risk Factor

None

### References

XREF USN:6727-2

### Plugin Information

Published: 2024/04/11, Modified: 2024/04/11

### Plugin Output

tcp/0

```
- Installed package : libnss3_2:3.68.2-0ubuntu1.2
- Fixed package     : libnss3_2:3.98-0ubuntu0.22.04.2
```

## 183197 - Ubuntu 22.04 ESM : iperf3 vulnerability (USN-6431-3)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 22.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6431-3 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-6431-3

### Solution

Update the affected iperf3, libiperf-dev and / or libiperf0 packages.

### Risk Factor

None

### References

XREF USN:6431-3

### Plugin Information

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

### Plugin Output

tcp/0

```
  - Installed package : iperf3_3.9-1+deb11u1build0.22.04.1
  - Fixed package     : iperf3_3.9-1+deb11u1ubuntu0.1~esm1

  - Installed package : libiperf0_3.9-1+deb11u1build0.22.04.1
  - Fixed package     : libiperf0_3.9-1+deb11u1ubuntu0.1~esm1


NOTE: The fixed ESM packages referenced in this plugin requires a
subscription to Ubuntu Pro to enable the ESM repositories.
```

## 198218 - Ubuntu Pro Subscription Detection

### Synopsis

The remote Ubuntu host has an active Ubuntu Pro subscription.

### Description

The remote Ubuntu host has an active Ubuntu Pro subscription.

### See Also

https://documentation.ubuntu.com/pro/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/05/31, Modified: 2024/07/05

### Plugin Output

tcp/0

```
This machine is NOT attached to an Ubuntu Pro subscription. However, it may have previously been
 attached.

The following details were gathered from /var/lib/ubuntu-advantage/status.json:

Binary Path                  : /var/lib/ubuntu-advantage
Binary Version               : 28.1~22.04
```

## 83303 - Unix / Linux - Local Users Information : Passwords Never Expire

### Synopsis

At least one local user has a password that never expires.

### Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

### Solution

Allow or require users to change their passwords regularly.

### Risk Factor

None

### Plugin Information

Published: 2015/05/10, Modified: 2023/11/27

### Plugin Output

tcp/0

```
Nessus found the following unlocked users with passwords that do not expire :
  - anapaya
```

## 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  0.2  0.0 167976 13796 ?        Ss    2023 909:49 /lib/systemd/systemd noquiet
 nosplash nofb --system --deserialize 48
root           2  0.0  0.0      0     0 ?        S     2023   0:08 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<    2023   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<    2023   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<    2023   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<    2023   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<    2023   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<    2023   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        S     2023   0:00 [rcu_tasks_rude_]
root          12  0.0  0.0      0     0 ?        S     2023   0:00 [rcu_tasks_trace]
root          13  0.0  0.0      0     0 ?        S     2023  17:40 [ksoftirqd/0]
root          14  0.0  0.0      0     0 ?        I     2023 315:21 [rcu_sched]
root          15  0.0  0.0      0     0 ?        S     2023   1:09 [migration/0]
root          16  0.0  0.0      0     0 ?        S     2023   0:00 [idle_inject/0]
root          18  0.0  0.0      0     0 ?        S     2023   0:00 [cpuhp/0]
root          19  0.0  0.0      0     0 ?        S     2023   0:00 [cpuhp/1]
root          20  0.0  0.0      0     0 ?        S     2023   0:00 [idle_inject/1]
root          21  0.0  0.0      0     0 ?        S     2023   1:42 [migration/1]
root          22  0.0  0.0      0     0 ?        S     2023   4:41 [ksoftirqd/1]
root          24  0.0  0.0      0     0 ?        I<    2023   0:00 [kworker/1:0H-events_highpri]
root          25  0.0  0.0      0     0 ?        S     2023   0:00 [cpuhp/2]
root          26  0.0  0.0      0     0 ?        S     2023   0:00 [idle_inject/2]
root          27  0.0  0.0      0     0 ?        S     2023   0:30 [migration/2]
root          28  0.0  0.0      0     [...]
```

## 152743 - Unix Software Discovery Commands Not Available

### Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

### Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.

Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

* Inadequate scan user permissions,

* Failed privilege escalation,

* Intermittent network disruption, or

* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

### Plugin Output

tcp/0

```
Failures in commands used to assess Unix software:

  unzip -v                    :
    sh: 1: unzip: not found


Account  : anapaya
Protocol : SSH
```

## 11154 - Unknown Service Detection: Banner Retrieval

### Synopsis

There is an unknown service running on the remote host.

### Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

### Plugin Output

tcp/30252

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port    : 30252
  Type    : spontaneous
  Banner :
0x00:  00 00 0C 04 00 00 00 00 00 00 05 00 00 40 00 00    .............@..
          0x10:  03 00 00 00 80                                        .....


Nessus detected the following process listening on this port :

/app/scion-all
```

## 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: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:

  Path    : /usr/bin/vim.tiny
  Version : 8.2

  Path    : /usr/bin/vim.basic
  Version : 8.2
```

## 91815 - Web Application Sitemap

### Synopsis

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

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

  - https://192.168.110.1/ui
  - https://192.168.110.1/ui/
  - https://192.168.110.1/ui/favicon.ico
  - https://192.168.110.1/ui/styles.f099f610cfe9907e.css

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

## 91815 - Web Application Sitemap

### Synopsis

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

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

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

  - http://192.168.110.1:42001/

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

## 10386 - Web Server No 404 Error Code Check

### Synopsis

The remote web server does not return 404 error codes.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

```
Unfortunately, Nessus has been unable to find a way to recognize this
page so some CGI-related checks have been disabled.
```

## 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.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: 2023/10/10, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.7.0
  Version            : 7.81.0
  Associated Package : libcurl4 7.81.0-1ubuntu1.16
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.7.0
  Version            : 7.81.0
  Associated Package : libcurl3-gnutls 7.81.0-1ubuntu1.16
  Managed by OS      : True
```

# 192.168.111.1

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 167 | 104 | 198 | 1 | 110 |

## Scan Information

Start time: Mon Aug 12 13:48:32 2024

End time: Mon Aug 12 14:11:42 2024

## Host Information

IP: 192.168.111.1

MAC Address: 02:42:7A:09:6D:69 AC:1F:6B:75:11:F5 00:1B:21:BE:34:50 00:1B:21:BE:34:52 AC:1F:6B:75:11:F4

OS: Linux Kernel 5.15.0-116-generic on Ubuntu 22.04

## Vulnerabilities

### 152782 - OpenSSL 1.1.1 < 1.1.1l Multiple Vulnerabilities

#### Synopsis

The remote service is affected by multiple vulnerabilities.

#### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1l. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1l advisory.

- ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the data and length fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the data field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in

the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack).

It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y). (CVE-2021-3712)

- In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the out parameter can be NULL and, on exit, the outlen parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the out parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k).

(CVE-2021-3711)

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

## See Also

http://www.nessus.org/u?4e69aead

http://www.nessus.org/u?77bbd34b

https://www.cve.org/CVERecord?id=CVE-2021-3711

https://www.cve.org/CVERecord?id=CVE-2021-3712

https://www.openssl.org/news/secadv/20210824.txt

## Solution

Upgrade to OpenSSL version 1.1.1l or later.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0679

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2021-3711 |
| CVE | CVE-2021-3712 |
| XREF | IAVA:2021-A-0395-S |

Plugin Information

Published: 2021/08/24, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

## 160477 - OpenSSL 1.1.1 < 1.1.1o Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).

Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd). (CVE-2022-1292)

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

### See Also

http://www.nessus.org/u?4d87f2b7

https://www.cve.org/CVERecord?id=CVE-2022-1292

https://www.openssl.org/news/secadv/20220503.txt

### Solution

Upgrade to OpenSSL version 1.1.1o or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

EPSS Score

0.1283

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-1292 |
| XREF | IAVA:2022-A-0186-S |

Plugin Information

Published: 2022/05/03, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

## 162420 - OpenSSL 1.1.1 < 1.1.1p Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). (CVE-2022-2068)

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

### See Also

http://www.nessus.org/u?33d5d7fb

https://www.cve.org/CVERecord?id=CVE-2022-2068

https://www.openssl.org/news/secadv/20220621.txt

### Solution

Upgrade to OpenSSL version 1.1.1p or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

EPSS Score

0.0932

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2022-2068 |

Plugin Information

Published: 2022/06/21, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

## 201084 - OpenSSL 1.1.1 < 1.1.1za Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 1.1.1za (premium support) (Affected since 1.1.1). (CVE-2024-5535)

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

See Also

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 1.1.1za or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-5535 |

Plugin Information

Published: 2024/06/27, Modified: 2024/07/03

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a3ddada6f511789b064e34c6e46f9a5b0cbd7035871f264c01c8ccbf1b990d04/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a61d71551040a2dbcdc9486754d5893a95daa05630eb3fe595ebaff12f2fedd1/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1za
```

## 201085 - OpenSSL 3.0.0 < 3.0.15 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.15. It is, therefore, affected by a vulnerability as referenced in the 3.0.15 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 1.1.1za (premium support) (Affected since 1.1.1). (CVE-2024-5535)

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

## See Also

http://www.nessus.org/u?8f2a60eb

https://www.cve.org/CVERecord?id=CVE-2024-5535

## Solution

Upgrade to OpenSSL version 3.0.15 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

6.0

## EPSS Score

0.0004

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2024-5535 |

## Plugin Information

Published: 2024/06/27, Modified: 2024/07/03

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.15
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.15
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.15
```

## 160473 - OpenSSL 3.0.0 < 3.0.3 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.3. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.3 advisory.

- The OPENSSL_LH_flush() function, which empties a hash table, contains a bug that breaks reuse of the memory occuppied by the removed hash table entries. This function is used when decoding certificates or keys. If a long lived process periodically decodes certificates or keys its memory usage will expand without bounds and the process might be terminated by the operating system causing a denial of service.

Also traversing the empty hash table entries will take increasingly more time. Typically such long lived processes might be TLS clients or TLS servers configured to accept client certificate authentication. The function was added in the OpenSSL 3.0 version thus older releases are not affected by the issue. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). (CVE-2022-1473)

- The OpenSSL 3.0 implementation of the RC4-MD5 ciphersuite incorrectly uses the AAD data as the MAC key.

This makes the MAC key trivially predictable. An attacker could exploit this issue by performing a man-in-the-middle attack to modify data being sent from one endpoint to an OpenSSL 3.0 recipient such that the modified data would still pass the MAC integrity check. Note that data sent from an OpenSSL 3.0 endpoint to a non-OpenSSL 3.0 endpoint will always be rejected by the recipient and the connection will fail at that point. Many application protocols require data to be sent from the client to the server first.

Therefore, in such a case, only an OpenSSL 3.0 server would be impacted when talking to a non-OpenSSL 3.0 client. If both endpoints are OpenSSL 3.0 then the attacker could modify data being sent in both directions. In this case both clients and servers could be affected, regardless of the application protocol. Note that in the absence of an attacker this bug means that an OpenSSL 3.0 endpoint communicating with a non-OpenSSL 3.0 endpoint will fail to complete the handshake when using this ciphersuite. The confidentiality of data is not impacted by this issue, i.e. an attacker cannot decrypt data that has been encrypted using this ciphersuite - they can only modify it. In order for this attack to work both endpoints must legitimately negotiate the RC4-MD5 ciphersuite. This ciphersuite is not compiled by default in OpenSSL 3.0, and is not available within the default provider or the default ciphersuite list. This ciphersuite will never be used if TLSv1.3 has been negotiated. In order for an OpenSSL 3.0 endpoint to use this ciphersuite the following must have occurred: 1) OpenSSL must have been compiled with the (non-default) compile time option enable-weak-ssl-ciphers 2) OpenSSL must have had the legacy provider explicitly loaded (either through application code or via configuration) 3) The ciphersuite must have been explicitly added to the ciphersuite list 4) The libssl security level must have been set to 0 (default is 1) 5) A version of SSL/TLS below TLSv1.3 must have been negotiated 6) Both endpoints must negotiate the RC4-MD5 ciphersuite in preference to any others that both endpoints have in common Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). (CVE-2022-1434)

- The function `OCSP_basic_verify` verifies the signer certificate on an OCSP response. In the case where the (non-default) flag OCSP_NOCHECKS is used then the response will be positive (meaning a successful verification) even in the case where the response signing certificate fails to verify. It is anticipated that most users of `OCSP_basic_verify` will not use the OCSP_NOCHECKS flag. In this case the `OCSP_basic_verify` function will return a negative value (indicating a fatal error) in the case of a certificate verification failure. The normal expected return value in this case would be 0. This issue also impacts the command line OpenSSL ocsp application. When verifying an ocsp response with the

-no_cert_checks option the command line application will report that the verification is successful even though it has in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). (CVE-2022-1343)

- The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n).

Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd). (CVE-2022-1292)

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://www.cve.org/CVERecord?id=CVE-2022-1292

https://www.cve.org/CVERecord?id=CVE-2022-1343

https://www.cve.org/CVERecord?id=CVE-2022-1434

https://www.cve.org/CVERecord?id=CVE-2022-1473

http://www.nessus.org/u?a704d771

http://www.nessus.org/u?ea9b1d96

https://www.openssl.org/news/secadv/20220503.txt

http://www.nessus.org/u?4e726fd8

http://www.nessus.org/u?7cec6b9a

## Solution

Upgrade to OpenSSL version 3.0.3 or later.

## Risk Factor

Critical

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

EPSS Score

0.1283

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-1292 |
| CVE | CVE-2022-1343 |
| CVE | CVE-2022-1434 |
| CVE | CVE-2022-1473 |
| XREF | IAVA:2022-A-0186-S |

Plugin Information

Published: 2022/05/03, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.3
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.3
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.3
```

## 162418 - OpenSSL 3.0.0 < 3.0.4 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.4. It is, therefore, affected by a vulnerability as referenced in the 3.0.4 advisory.

- In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze). (CVE-2022-2068)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-2068

http://www.nessus.org/u?8c2076d9

https://www.openssl.org/news/secadv/20220621.txt

### Solution

Upgrade to OpenSSL version 3.0.4 or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

7.4

EPSS Score

0.0932

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-2068 |
| XREF | IAVA:2022-A-0257-S |

Plugin Information

Published: 2022/06/21, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.4
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.4
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
```

```
    Fixed version     : 3.0.4
```

## 162720 - OpenSSL 3.0.0 < 3.0.5 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.5. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.5 advisory.

- The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such machines and memory corruption will happen during the computation. As a consequence of the memory corruption an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048 bit RSA private keys running on machines supporting AVX512IFMA instructions of the X86_64 architecture are affected by this issue. (CVE-2022-2274)

- AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of in place encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). (CVE-2022-2097)

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

### See Also

http://www.nessus.org/u?05ef5c2c

http://www.nessus.org/u?58b324e2

https://www.openssl.org/news/secadv/20220705.txt

https://www.cve.org/CVERecord?id=CVE-2022-2097

https://www.cve.org/CVERecord?id=CVE-2022-2274

### Solution

Upgrade to OpenSSL version 3.0.5 or later.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0224

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-2097 |
| CVE | CVE-2022-2274 |
| XREF | IAVA:2022-A-0265-S |

Plugin Information

Published: 2022/07/05, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version     : 3.0.5
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
```

```
  Reported version : 3.0.2
  Fixed version    : 3.0.5
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.5
```

## 201082 - OpenSSL 3.1.0 < 3.1.7 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.7. It is, therefore, affected by a vulnerability as referenced in the 3.1.7 advisory.

- Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash.

In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a no overlap response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. Found by Joseph Birr-Pixton. Thanks to David Benjamin (Google). Fix developed by Matt Caswell. Fixed in OpenSSL 3.3.2 (Affected since 3.3.0). (CVE-2024-5535)

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

See Also

http://www.nessus.org/u?f87142a6

https://www.cve.org/CVERecord?id=CVE-2024-5535

Solution

Upgrade to OpenSSL version 3.1.7 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-5535 |

Plugin Information

Published: 2024/06/27, Modified: 2024/07/03

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1a76dcd30f60c22fe5111760cfbbd44ab2c1050fda33256282e749cd48a48759/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.7
```

## 182308 - OpenSSL SEoL (1.1.1.x)

### Synopsis

An unsupported version of OpenSSL is installed on the remote host.

### Description

According to its version, OpenSSL is 1.1.1.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

### See Also

https://www.openssl.org/blog/blog/2023/09/11/eol-111/

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

https://www.openssl.org/news/vulnerabilities-1.1.1.html

### Solution

Upgrade to a version of OpenSSL that is currently supported.

### Risk Factor

Critical

### CVSS v3.0 Base Score

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

### CVSS v2.0 Base Score

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

### Plugin Information

Published: 2023/09/29, Modified: 2024/05/31

### Plugin Output

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
```

```
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Installed version                       : 1.1.1w
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Installed version                       : 1.1.1w
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Installed version                       : 1.1.1k
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1w
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Installed version                   : 1.1.1w
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
a3ddada6f511789b064e34c6e46f9a5b0cbd7035871f264c01c8ccbf1b990d04/diff/usr/bin/openssl
  Installed version                   : 1.1.1w
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
a61d71551040a2dbcdc9486754d5893a95daa05630eb3fe595ebaff12f2fedd1/diff/usr/bin/openssl
  Installed version                   : 1.1.1w
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                   : 1.1.1k
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/bin/openssl
  Installed version                   : 1.1.1w
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                   : 1.1.1w
  Security End of Life                : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                   : 1.1.1w
  Security End of Life                : September 11, 2023
```

```
   Time since Security End of Life (Est.) : >= 6 months
```

## 204924 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenSSL vulnerabilities (USN-6937-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6937-1 advisory.

It was discovered that OpenSSL incorrectly handled TLSv1.3 sessions when certain non-default TLS server configurations were in use. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. (CVE-2024-2511)

It was discovered that OpenSSL incorrectly handled checking excessively long DSA keys or parameters. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-4603)

William Ahern discovered that OpenSSL incorrectly handled certain memory operations in a rarely-used API.

A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-4741)

Joseph Birr-Pixton discovered that OpenSSL incorrectly handled calling a certain API with an empty supported client protocols buffer. A remote attacker could possibly use this issue to obtain sensitive information, or cause OpenSSL to crash, resulting in a denial of service. (CVE-2024-5535)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6937-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0004

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4603 |
| CVE | CVE-2024-4741 |
| CVE | CVE-2024-5535 |
| XREF | IAVA:2024-A-0208-S |
| XREF | IAVA:2024-A-0321 |
| XREF | USN:6937-1 |

Plugin Information

Published: 2024/07/31, Modified: 2024/07/31

Plugin Output

tcp/0

```
  - Installed package : libssl3_3.0.2-0ubuntu1.16
  - Fixed package     : libssl3_3.0.2-0ubuntu1.17

  - Installed package : openssl_3.0.2-0ubuntu1.16
  - Fixed package     : openssl_3.0.2-0ubuntu1.17
```

## 158974 - OpenSSL 1.1.1 < 1.1.1n Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self- signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc). (CVE-2022-0778)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-0778

http://www.nessus.org/u?2a52134e

https://www.openssl.org/news/secadv/20220315.txt

### Solution

Upgrade to OpenSSL version 1.1.1n or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.1

EPSS Score

0.0134

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-0778 |
| XREF | IAVA:2022-A-0121-S |

Plugin Information

Published: 2022/03/16, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
```

```
    Fixed version    : 1.1.1n
```

## 171079 - OpenSSL 1.1.1 < 1.1.1t Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1t. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1t advisory.

- There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName.

X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network. (CVE-2023-0286)

- The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected. (CVE-2023-0215)

- The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the name (e.g.

CERTIFICATE), any header data and the payload data. If the function succeeds then the name_out, header and data arguments are populated with pointers to buffers containing the relevant decoded data.

The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the

PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue. (CVE-2022-4450)

- A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption.

The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection. (CVE-2022-4304)

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://www.cve.org/CVERecord?id=CVE-2023-0286

https://www.openssl.org/news/secadv/20230207.txt

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

https://www.cve.org/CVERecord?id=CVE-2023-0215

https://www.cve.org/CVERecord?id=CVE-2022-4450

https://www.cve.org/CVERecord?id=CVE-2022-4304

## Solution

Upgrade to OpenSSL version 1.1.1t or later.

## 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:N/A:H)

## CVSS v3.0 Temporal Score

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

## VPR Score

6.0

## EPSS Score

0.0049

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2022-4304 |
| CVE | CVE-2022-4450 |
| CVE | CVE-2023-0215 |
| CVE | CVE-2023-0286 |

### Plugin Information

Published: 2023/02/07, Modified: 2024/06/07

### Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

## 181288 - OpenSSL 1.1.1 < 1.1.1w Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroized so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000 The FIPS provider is not affected by this issue.

(CVE-2023-4807)

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

### See Also

http://www.nessus.org/u?05c4bf30

https://www.cve.org/CVERecord?id=CVE-2023-4807

https://www.openssl.org/news/secadv/20230908.txt

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

### Solution

Upgrade to OpenSSL version 1.1.1w or later.

### Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-4807 |
| XREF | IAVA:2023-A-0462-S |

Plugin Information

Published: 2023/09/12, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

## 181289 - OpenSSL 3.0.0 < 3.0.11 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.11. It is, therefore, affected by a vulnerability as referenced in the 3.0.11 advisory.

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroized so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000 The FIPS provider is not affected by this issue.

(CVE-2023-4807)

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

### See Also

http://www.nessus.org/u?eeb05f22

https://www.cve.org/CVERecord?id=CVE-2023-4807

https://www.openssl.org/news/secadv/20230908.txt

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

### Solution

Upgrade to OpenSSL version 3.0.11 or later.

### Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-4807 |
| XREF | IAVA:2023-A-0462-S |

Plugin Information

Published: 2023/09/12, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.11
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.11
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.11
```

## 183891 - OpenSSL 3.0.0 < 3.0.12 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.12. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.12 advisory.

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

- Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths.

This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers.

Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the keylen parameter or the IV length, via the ivlen parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.

(CVE-2023-5363)

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

## See Also

http://www.nessus.org/u?608327d1

http://www.nessus.org/u?71a978e4

https://www.cve.org/CVERecord?id=CVE-2023-5363

https://www.cve.org/CVERecord?id=CVE-2023-6129

## Solution

Upgrade to OpenSSL version 3.0.12 or later.

## Risk Factor

High

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

5.0

## EPSS Score

0.0016

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-5363 |
| CVE | CVE-2023-6129 |
| XREF | IAVA:2023-A-0582-S |

## Plugin Information

Published: 2023/10/25, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.12
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.12
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.12
```

## 166047 - OpenSSL 3.0.0 < 3.0.6 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.6. It is, therefore, affected by a vulnerability as referenced in the 3.0.6 advisory.

- OpenSSL supports creating a custom cipher via the legacy EVP_CIPHER_meth_new() function and associated function calls. This function was deprecated in OpenSSL 3.0 and application authors are instead encouraged to use the new provider mechanism in order to implement custom ciphers. OpenSSL versions 3.0.0 to 3.0.5 incorrectly handle legacy custom ciphers passed to the EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() and EVP_CipherInit_ex2() functions (as well as other similarly named encryption and decryption initialisation functions). Instead of using the custom cipher directly it incorrectly tries to fetch an equivalent cipher from the available providers. An equivalent cipher is found based on the NID passed to EVP_CIPHER_meth_new(). This NID is supposed to represent the unique NID for a given cipher. However it is possible for an application to incorrectly pass NID_undef as this value in the call to EVP_CIPHER_meth_new(). When NID_undef is used in this way the OpenSSL encryption/decryption initialisation function will match the NULL cipher as being equivalent and will fetch this from the available providers.

This will succeed if the default provider has been loaded (or if a third party provider has been loaded that offers this cipher). Using the NULL cipher means that the plaintext is emitted as the ciphertext.

Applications are only affected by this issue if they call EVP_CIPHER_meth_new() using NID_undef and subsequently use it in a call to an encryption/decryption initialisation function. Applications that only use SSL/TLS are not impacted by this issue. Fixed in OpenSSL 3.0.6 (Affected 3.0.0-3.0.5). (CVE-2022-3358)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-3358

http://www.nessus.org/u?ca4894f6

https://www.openssl.org/news/secadv/20221011.txt

### Solution

Upgrade to OpenSSL version 3.0.6 or later.

### Risk Factor

High

### CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-3358 |
| XREF | IAVA:2022-A-0415-S |

Plugin Information

Published: 2022/10/11, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.6
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
```

```
  Fixed version    : 3.0.6
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.6
```

## 166773 - OpenSSL 3.0.0 < 3.0.7 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.7. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.7 advisory.

- A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed a malicious certificate or for an application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address in a certificate to overflow an arbitrary number of bytes containing the `.' character (decimal 46) on the stack. This buffer overflow could result in a crash (causing a denial of service). In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. (CVE-2022-3786)

- A buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. An attacker can craft a malicious email address to overflow four attacker-controlled bytes on the stack. This buffer overflow could result in a crash (causing a denial of service) or potentially remote code execution. Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler. Pre-announcements of CVE-2022-3602 described this issue as CRITICAL. Further analysis based on some of the mitigating factors described above have led this to be downgraded to HIGH. Users are still encouraged to upgrade to a new version as soon as possible. In a TLS client, this can be triggered by connecting to a malicious server.

In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. Fixed in OpenSSL 3.0.7 (Affected 3.0.0,3.0.1,3.0.2,3.0.3,3.0.4,3.0.5,3.0.6). (CVE-2022-3602)

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://www.openssl.org/news/secadv/20221101.txt

http://www.nessus.org/u?b279f369

http://www.nessus.org/u?ba8a3e9f

https://www.cve.org/CVERecord?id=CVE-2022-3602

https://www.cve.org/CVERecord?id=CVE-2022-3786

### Solution

Upgrade to OpenSSL version 3.0.7 or later.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.1016

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-3602 |
| CVE | CVE-2022-3786 |
| XREF | IAVA:2022-A-0452-S |
| XREF | CEA-ID:CEA-2022-0036 |

Plugin Information

Published: 2022/11/01, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
```

```
  Fixed version    : 3.0.7
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.7
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.7
```

## 168829 - OpenSSL 3.0.0 < 3.0.8 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.8. It is, therefore, affected by a denial of service (DoS) vulnerability. If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the -policy argument to the command line utilities or by calling either X509_VERIFY_PARAM_add0_policy() or X509_VERIFY_PARAM_set1_policies() functions.

- There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName.

X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network. (CVE-2023-0286)

- If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the

`-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()'

function. Update (31 March 2023): The description of the policy processing enablement was corrected based on CVE-2023-0466. (CVE-2022-3996)

- A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. The read buffer overrun might result in a crash which could lead to a denial of service attack. In theory it could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext) although we are not aware of any working exploit leading to memory contents disclosure as of the time of release of this advisory. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects. (CVE-2022-4203)

- A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption.

The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number

of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection. (CVE-2022-4304)

- The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the name (e.g.

CERTIFICATE), any header data and the payload data. If the function succeeds then the name_out, header and data arguments are populated with pointers to buffers containing the relevant decoded data.

The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue. (CVE-2022-4450)

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://www.cve.org/CVERecord?id=CVE-2023-0401

https://www.openssl.org/news/secadv/20230207.txt

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

https://www.cve.org/CVERecord?id=CVE-2023-0286

https://www.cve.org/CVERecord?id=CVE-2023-0217

https://www.cve.org/CVERecord?id=CVE-2023-0216

https://www.cve.org/CVERecord?id=CVE-2023-0215

https://www.cve.org/CVERecord?id=CVE-2022-4450

https://www.cve.org/CVERecord?id=CVE-2022-4304

https://www.cve.org/CVERecord?id=CVE-2022-4203

## Solution

Upgrade to OpenSSL version 3.0.8 or later.

## 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:N/A:H)

## CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0049

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-3996 |
| CVE | CVE-2022-4203 |
| CVE | CVE-2022-4304 |
| CVE | CVE-2022-4450 |
| CVE | CVE-2023-0215 |
| CVE | CVE-2023-0216 |
| CVE | CVE-2023-0217 |
| CVE | CVE-2023-0286 |
| CVE | CVE-2023-0401 |
| XREF | IAVA:2022-A-0518-S |

Plugin Information

Published: 2022/12/15, Modified: 2024/01/08

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

## 183890 - OpenSSL 3.1.0 < 3.1.4 Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.4. It is, therefore, affected by a vulnerability as referenced in the 3.1.4 advisory.

- Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths.

This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers.

Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling EVP_EncryptInit_ex2(), EVP_DecryptInit_ex2() or EVP_CipherInit_ex2() the provided OSSL_PARAM array is processed after the key and IV have been established. Any alterations to the key length, via the keylen parameter or the IV length, via the ivlen parameter, within the OSSL_PARAM array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.

(CVE-2023-5363)

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

### See Also

http://www.nessus.org/u?442518e0

https://www.cve.org/CVERecord?id=CVE-2023-5363

https://www.openssl.org/news/secadv/20231024.txt

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

### Solution

Upgrade to OpenSSL version 3.1.4 or later.

### Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0011

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5363 |
| XREF | IAVA:2023-A-0582-S |

Plugin Information

Published: 2023/10/25, Modified: 2024/03/08

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1a76dcd30f60c22fe5111760cfbbd44ab2c1050fda33256282e749cd48a48759/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.4
```

## 205195 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos vulnerabilities (USN-6947-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6947-1 advisory.

It was discovered that Kerberos incorrectly handled GSS message tokens where an unwrapped token could appear to be truncated. An attacker could possibly use this issue to cause a denial of service.

(CVE-2024-37370)

It was discovered that Kerberos incorrectly handled GSS message tokens when sent a token with invalid length fields. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-37371)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6947-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.2

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2024-37370 |
| CVE | CVE-2024-37371 |
| XREF | USN:6947-1 |

### Plugin Information

Published: 2024/08/08, Modified: 2024/08/08

### Plugin Output

tcp/0

```
- Installed package : libgssapi-krb5-2_1.19.2-2ubuntu0.3
- Fixed package     : libgssapi-krb5-2_1.19.2-2ubuntu0.4

- Installed package : libk5crypto3_1.19.2-2ubuntu0.3
- Fixed package     : libk5crypto3_1.19.2-2ubuntu0.4

- Installed package : libkrb5-3_1.19.2-2ubuntu0.3
- Fixed package     : libkrb5-3_1.19.2-2ubuntu0.4

- Installed package : libkrb5support0_1.19.2-2ubuntu0.3
- Fixed package     : libkrb5support0_1.19.2-2ubuntu0.4
```

## 185739 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : pip vulnerabilities (USN-6473-2)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6473-2 advisory.

- urllib3 before 1.24.2 does not remove the authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the authorization header to be exposed to unintended hosts or transmitted in cleartext. NOTE: this issue exists because of an incomplete fix for CVE-2018-20060 (which was case-sensitive). (CVE-2018-25091)

- urllib3 is a user-friendly HTTP client library for Python. urllib3 doesn't treat the `Cookie` HTTP header special or provide any helpers for managing cookies over HTTP, that is the responsibility of the user.

However, it is possible for a user to specify a `Cookie` header and unknowingly leak information via HTTP redirects to a different origin if that user doesn't disable redirects explicitly. This issue has been patched in urllib3 version 1.26.17 or 2.0.5. (CVE-2023-43804)

- urllib3 is a user-friendly HTTP client library for Python. urllib3 previously wouldn't remove the HTTP request body when an HTTP redirect response using status 301, 302, or 303 after the request had its method changed from one that could accept a request body (like `POST`) to `GET` as is required by HTTP RFCs.

Although this behavior is not specified in the section for redirects, it can be inferred by piecing together information from different sections and we have observed the behavior in other major HTTP client implementations like curl and web browsers. Because the vulnerability requires a previously trusted service to become compromised in order to have an impact on confidentiality we believe the exploitability of this vulnerability is low. Additionally, many users aren't putting sensitive data in HTTP request bodies, if this is the case then this vulnerability isn't exploitable. Both of the following conditions must be true to be affected by this vulnerability: 1. Using urllib3 and submitting sensitive information in the HTTP request body (such as form data or JSON) and 2. The origin service is compromised and starts redirecting using 301, 302, or 303 to a malicious peer or the redirected-to service becomes compromised.

This issue has been addressed in versions 1.26.18 and 2.0.7 and users are advised to update to resolve this issue. Users unable to update should disable redirects for services that aren't expecting to respond with redirects with `redirects=False` and disable automatic redirects with `redirects=False` and handle 301, 302, and 303 redirects manually by stripping the HTTP request body. (CVE-2023-45803)

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://ubuntu.com/security/notices/USN-6473-2

### Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0008

CVSS v2.0 Base Score

8.5 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2018-25091 |
| CVE | CVE-2023-43804 |
| CVE | CVE-2023-45803 |
| XREF | USN:6473-2 |

Plugin Information

Published: 2023/11/15, Modified: 2023/11/15

Plugin Output

tcp/0

```
- Installed package : python3-pip_22.0.2+dfsg-1ubuntu0.3
- Fixed package     : python3-pip_22.0.2+dfsg-1ubuntu0.4
```

## 195216 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6768-1 advisory.

- An issue was discovered in GNOME GLib before 2.78.5, and 2.79.x and 2.80.x before 2.80.1. When a GDBus- based client subscribes to signals from a trusted system service such as NetworkManager on a shared computer, other users of the same computer can send spoofed D-Bus signals that the GDBus-based client will wrongly interpret as having been sent by the trusted system service. This could lead to the GDBus-based client behaving incorrectly, with an application-dependent impact. (CVE-2024-34397)

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

### See Also

https://ubuntu.com/security/notices/USN-6768-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

2.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-34397 |
| XREF | USN:6768-1 |

Plugin Information

Published: 2024/05/09, Modified: 2024/05/09

Plugin Output

tcp/0

```
  - Installed package : libglib2.0-data_2.72.4-0ubuntu2.2
  - Fixed package     : libglib2.0-data_2.72.4-0ubuntu2.3
```

## 204989 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-6944-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6944-1 advisory.

Dov Murik discovered that curl incorrectly handled parsing ASN.1 Generalized Time fields. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly obtain sensitive memory contents.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-6944-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.9

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### STIG Severity

I

### References

| | |
|---|---|
| CVE | CVE-2024-7264 |
| XREF | IAVA:2024-A-0457 |
| XREF | USN:6944-1 |

### Plugin Information

Published: 2024/08/05, Modified: 2024/08/05

### Plugin Output

tcp/0

```
- Installed package : curl_7.81.0-1ubuntu1.16
- Fixed package     : curl_7.81.0-1ubuntu1.17

- Installed package : libcurl3-gnutls_7.81.0-1ubuntu1.16
- Fixed package     : libcurl3-gnutls_7.81.0-1ubuntu1.17

- Installed package : libcurl4_7.81.0-1ubuntu1.16
- Fixed package     : libcurl4_7.81.0-1ubuntu1.17
```

## 204913 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6923-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6923-1 advisory.

Benedict Schlter, Supraja Sridhara, Andrin Bertschi, and Shweta Shinde discovered that an untrusted hypervisor could inject malicious #VC interrupts and compromise the security guarantees of AMD SEV-SNP.

This flaw is known as WeSee. A local attacker in control of the hypervisor could use this to expose sensitive information or possibly execute arbitrary code in the trusted execution environment.

(CVE-2024-25742)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- TTY drivers;

- SMB network file system;

- Netfilter;

- Bluetooth subsystem; (CVE-2024-26886, CVE-2024-26952, CVE-2023-52752, CVE-2024-27017, CVE-2024-36016)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6923-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-52752 |
| CVE | CVE-2024-25742 |
| CVE | CVE-2024-26886 |
| CVE | CVE-2024-26952 |
| CVE | CVE-2024-27017 |
| CVE | CVE-2024-36016 |
| XREF | USN:6923-1 |

Plugin Information

Published: 2024/07/31, Modified: 2024/07/31

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-116-generic does not meet the minimum fixed level of 5.15.0-117-
generic for this advisory.
```

## 189773 - Ubuntu 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-6616-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6616-1 advisory.

- A vulnerability was found in openldap. This security flaw causes a null pointer dereference in ber_memalloc_x() function. (CVE-2023-2953)

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

### See Also

https://ubuntu.com/security/notices/USN-6616-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0039

### CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-2953 |
| XREF | USN:6616-1 |

## Plugin Information

Published: 2024/01/30, Modified: 2024/01/30

## Plugin Output

tcp/0

```
  - Installed package : libldap-common_2.5.16+dfsg-0ubuntu0.22.04.1
  - Fixed package     : libldap-common_2.5.16+dfsg-0ubuntu0.22.04.2
```

## 204858 - Ubuntu 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-6928-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6928-1 advisory.

It was discovered that the Python ssl module contained a memory race condition when handling the APIs to obtain the CA certificates and certificate store statistics. This could possibly result in applications obtaining wrong results, leading to various SSL issues. (CVE-2024-0397)

It was discovered that the Python ipaddress module contained incorrect information about which IP address ranges were considered private or globally reachable. This could possibly result in applications applying incorrect security policies. (CVE-2024-4032)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6928-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.0

### EPSS Score

0.0005

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2024-0397 |
| CVE | CVE-2024-4032 |
| XREF | USN:6928-1 |

## Plugin Information

Published: 2024/07/30, Modified: 2024/07/30

## Plugin Output

tcp/0

```
- Installed package : libpython3.10_3.10.12-1~22.04.4
- Fixed package     : libpython3.10_3.10.12-1~22.04.5

- Installed package : libpython3.10-minimal_3.10.12-1~22.04.4
- Fixed package     : libpython3.10-minimal_3.10.12-1~22.04.5

- Installed package : libpython3.10-stdlib_3.10.12-1~22.04.4
- Fixed package     : libpython3.10-stdlib_3.10.12-1~22.04.5

- Installed package : python3.10_3.10.12-1~22.04.4
- Fixed package     : python3.10_3.10.12-1~22.04.5

- Installed package : python3.10-minimal_3.10.12-1~22.04.4
- Fixed package     : python3.10-minimal_3.10.12-1~22.04.5
```

## 157228 - OpenSSL 1.1.1 < 1.1.1m Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 3.0.1 (Affected 3.0.0). Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). Fixed in OpenSSL 1.0.2zc- dev (Affected 1.0.2-1.0.2zb). (CVE-2021-4160)

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

### See Also

http://www.nessus.org/u?da5b5058

https://www.cve.org/CVERecord?id=CVE-2021-4160

https://www.openssl.org/news/secadv/20220128.txt

### Solution

Upgrade to OpenSSL version 1.1.1m or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0042

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE CVE-2021-4160

Plugin Information

Published: 2022/01/28, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version     : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

## 162721 - OpenSSL 1.1.1 < 1.1.1q Vulnerability

### Synopsis

The remote service is affected by a vulnerability.

### Description

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

- AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of in place encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). (CVE-2022-2097)

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

### See Also

https://www.cve.org/CVERecord?id=CVE-2022-2097

http://www.nessus.org/u?ec8857b4

https://www.openssl.org/news/secadv/20220705.txt

### Solution

Upgrade to OpenSSL version 1.1.1q or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

2.2

### EPSS Score

0.0037

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2022-2097 |
| XREF | IAVA:2022-A-0265-S |

Plugin Information

Published: 2022/07/05, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

## 173260 - OpenSSL 1.1.1 < 1.1.1u Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1u. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1u advisory.

- Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit.

OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(n^2) with 'n'

being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low. (CVE-2023-2650)

- Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0465)

- The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification.

As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable

the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument.

Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.

(CVE-2023-0466)

- A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0464)

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

## See Also

http://www.nessus.org/u?2b09deba

http://www.nessus.org/u?f976d208

https://www.openssl.org/news/secadv/20230328.txt

https://www.openssl.org/news/secadv/20230530.txt

https://www.openssl.org/policies/general/security-policy.html

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

http://www.nessus.org/u?1b17844f

http://www.nessus.org/u?0f79dd95

https://www.openssl.org/news/secadv/20230322.txt

https://www.cve.org/CVERecord?id=CVE-2023-0464

https://www.cve.org/CVERecord?id=CVE-2023-0464

https://www.cve.org/CVERecord?id=CVE-2023-0465

https://www.cve.org/CVERecord?id=CVE-2023-0466

https://www.cve.org/CVERecord?id=CVE-2023-2650

## Solution

Upgrade to OpenSSL version 1.1.1u or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.003

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0465 |
| CVE | CVE-2023-0466 |
| CVE | CVE-2023-2650 |
| XREF | IAVA:2023-A-0158-S |

Plugin Information

Published: 2023/03/22, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
```

```
  Path              : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

## 178475 - OpenSSL 1.1.1 < 1.1.1v Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1v. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1v advisory.

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check().

Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the -check option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3817)

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3446)

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

### See Also

http://www.nessus.org/u?34493939

http://www.nessus.org/u?4c441c47

https://www.openssl.org/news/secadv/20230719.txt

https://www.openssl.org/news/secadv/20230731.txt

https://www.openssl.org/policies/secpolicy.html
https://www.cve.org/CVERecord?id=CVE-2023-3446
https://www.cve.org/CVERecord?id=CVE-2023-3817

## Solution

Upgrade to OpenSSL version 1.1.1v or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

2.2

## EPSS Score

0.0043

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-3446 |
| CVE | CVE-2023-3817 |
| XREF | IAVA:2023-A-0398-S |

## Plugin Information

Published: 2023/07/19, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

## 184811 - OpenSSL 1.1.1 < 1.1.1x Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

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

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

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

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

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

### See Also

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

https://www.cve.org/CVERecord?id=CVE-2024-0727

### Solution

Upgrade to OpenSSL version 1.1.1x or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5678 |
| CVE | CVE-2024-0727 |
| XREF | IAVA:2024-A-0121-S |

Plugin Information

Published: 2023/11/07, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a3ddada6f511789b064e34c6e46f9a5b0cbd7035871f264c01c8ccbf1b990d04/diff/usr/bin/openssl
  Reported version : 1.1.1w
```

```
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a61d71551040a2dbcdc9486754d5893a95daa05630eb3fe595ebaff12f2fedd1/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

## 192965 - OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 1.1.1y. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1y advisory.

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4741

### Solution

Upgrade to OpenSSL version 1.1.1y or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### STIG Severity

I

### References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4741 |
| XREF | IAVA:2024-A-0208-S |

### Plugin Information

Published: 2024/04/08, Modified: 2024/06/07

### Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Reported version : 1.1.1k
```

```
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a3ddada6f511789b064e34c6e46f9a5b0cbd7035871f264c01c8ccbf1b990d04/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a61d71551040a2dbcdc9486754d5893a95daa05630eb3fe595ebaff12f2fedd1/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

## 178478 - OpenSSL 3.0.0 < 3.0.10 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.10. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.10 advisory.

- Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary:

Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue. (CVE-2023-3446)

- Issue summary: The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence. Impact summary: Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be mislead by removing adding or reordering such empty entries as these are ignored by the OpenSSL implementation. We are currently unaware of any such applications. The AES-SIV algorithm allows for authentication of multiple associated data entries along with the encryption. To authenticate empty data the application has to call EVP_EncryptUpdate() (or EVP_CipherUpdate()) with NULL pointer as the output buffer and 0 as the input buffer length. The AES-SIV implementation in OpenSSL just returns success for such a call instead of performing the associated data authentication operation. The empty data thus will not be authenticated. As this issue does not affect non-empty associated data authentication and we expect it to be rare for an application to use empty associated data entries this is qualified as Low severity issue. (CVE-2023-2975)

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

### See Also

http://www.nessus.org/u?92592957

http://www.nessus.org/u?e3173aec

https://www.openssl.org/news/secadv/20230719.txt

https://www.openssl.org/news/secadv/20230731.txt

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

http://www.nessus.org/u?a7b15686

https://www.openssl.org/news/secadv/20230714.txt
https://www.cve.org/CVERecord?id=CVE-2023-2975
https://www.cve.org/CVERecord?id=CVE-2023-3446
https://www.cve.org/CVERecord?id=CVE-2023-3817

## Solution

Upgrade to OpenSSL version 3.0.10 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

2.2

## EPSS Score

0.0043

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-2975 |
| CVE | CVE-2023-3446 |
| CVE | CVE-2023-3817 |
| XREF | IAVA:2023-A-0398-S |

## Plugin Information

Published: 2023/07/19, Modified: 2024/01/08

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.10
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.10
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.10
```

## 185160 - OpenSSL 3.0.0 < 3.0.13 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.13. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.13 advisory.

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

- Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary:

Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2023-6237)

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

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

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

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

## See Also

http://www.nessus.org/u?02bfb3df

http://www.nessus.org/u?71a978e4

http://www.nessus.org/u?ccacbb1d

http://www.nessus.org/u?fc067b0a

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

https://www.cve.org/CVERecord?id=CVE-2023-6129

https://www.cve.org/CVERecord?id=CVE-2023-6237

https://www.cve.org/CVERecord?id=CVE-2024-0727

## Solution

Upgrade to OpenSSL version 3.0.13 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5678 |
| CVE | CVE-2023-6129 |
| CVE | CVE-2023-6237 |
| CVE | CVE-2024-0727 |
| XREF | IAVA:2024-A-0121-S |

Plugin Information

Published: 2023/11/07, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.13
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.13
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.13
```

## 192966 - OpenSSL 3.0.0 < 3.0.14 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.14. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.14 advisory.

- Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary:

Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2024-4603)

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware

of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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

### See Also

http://www.nessus.org/u?141a6242

http://www.nessus.org/u?2cbb1fb1

http://www.nessus.org/u?8409be15

https://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4741

### Solution

Upgrade to OpenSSL version 3.0.14 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.6

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4603 |
| CVE | CVE-2024-4741 |
| XREF | IAVA:2024-A-0208-S |

## Plugin Information

Published: 2024/04/08, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.14
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.14
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.14
```

## 173263 - OpenSSL 3.0.0 < 3.0.9 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.0.9. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.9 advisory.

- The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification.

As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument.

Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.

(CVE-2023-0466)

- A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0464)

- Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function. (CVE-2023-0465)

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

### See Also

http://www.nessus.org/u?91a43679

https://www.cve.org/CVERecord?id=CVE-2023-0465

https://www.openssl.org/news/secadv/20230328.txt

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

http://www.nessus.org/u?a5af6e0b

https://www.cve.org/CVERecord?id=CVE-2023-0466

http://www.nessus.org/u?0fd4fada

https://www.cve.org/CVERecord?id=CVE-2023-0464
https://www.openssl.org/news/secadv/20230322.txt

## Solution

Upgrade to OpenSSL version 3.0.9 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

4.4

## EPSS Score

0.003

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0464 |
| CVE | CVE-2023-0465 |
| CVE | CVE-2023-0466 |
| XREF | IAVA:2023-A-0158-S |

## Plugin Information

Published: 2023/03/22, Modified: 2024/01/08

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1e1a1f3d3d2d1281812add826d4259b548f19d75f7fb1b1d7860fde61f10e5a/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f96cbab491579ed5bc56fe220573cc0c2f7f0634bbf9579a191729d3e067a1a8/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

## 185161 - OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.5. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.5 advisory.

- Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are:

PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. (CVE-2024-0727)

- Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary:

Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2023-6237)

- Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used.

This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. (CVE-2023-6129)

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

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

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

## See Also

http://www.nessus.org/u?0a42ec4e

http://www.nessus.org/u?950a9188

http://www.nessus.org/u?aca829a1

http://www.nessus.org/u?d086a7ea

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

https://www.cve.org/CVERecord?id=CVE-2023-6129

https://www.cve.org/CVERecord?id=CVE-2023-6237

https://www.cve.org/CVERecord?id=CVE-2024-0727

## Solution

Upgrade to OpenSSL version 3.1.5 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

VPR Score

5.0

EPSS Score

0.0023

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-5678 |
| CVE | CVE-2023-6129 |
| CVE | CVE-2023-6237 |
| CVE | CVE-2024-0727 |
| XREF | IAVA:2024-A-0121-S |

Plugin Information

Published: 2023/11/07, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1a76dcd30f60c22fe5111760cfbbd44ab2c1050fda33256282e749cd48a48759/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.5
```

## 192974 - OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities

### Synopsis

The remote service is affected by multiple vulnerabilities.

### Description

The version of OpenSSL installed on the remote host is prior to 3.1.6. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.1.6 advisory.

- Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary:

Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (`p` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey and pkeyparam command line applications when using the `-check` option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue. (CVE-2024-4603)

- Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

(CVE-2024-2511)

- Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware

of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Found by William Ahern (Akamai). Fix developed by Matt Caswell. Fix developed by Watson Ladd (Akamai). Fixed in OpenSSL 3.3.1 (Affected since 3.3.0). (CVE-2024-4741)

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

## See Also

http://www.nessus.org/u?5ee92eab

http://www.nessus.org/u?6f15218c

http://www.nessus.org/u?f40bd907

https://www.cve.org/CVERecord?id=CVE-2024-2511

https://www.cve.org/CVERecord?id=CVE-2024-4603

https://www.cve.org/CVERecord?id=CVE-2024-4741

## Solution

Upgrade to OpenSSL version 3.1.6 or later.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

3.6

## EPSS Score

0.0004

## CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4603 |
| CVE | CVE-2024-4741 |
| XREF | IAVA:2024-A-0208-S |

## Plugin Information

Published: 2024/04/08, Modified: 2024/06/07

## Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1a76dcd30f60c22fe5111760cfbbd44ab2c1050fda33256282e749cd48a48759/diff/lib/libcrypto.so.3
  Reported version : 3.1.3
  Fixed version    : 3.1.6
```

## 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/443/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=Caddy Local Authority - ECC Intermediate
|-Issuer  : CN=Caddy Local Authority - 2023 ECC Root
```

## 190598 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6640-1 advisory.

- A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.

(CVE-2023-4641)

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

### See Also

https://ubuntu.com/security/notices/USN-6640-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:C/I:N/A:N)

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2023-4641 |
| XREF | USN:6640-1 |

### Plugin Information

Published: 2024/02/15, Modified: 2024/02/15

### Plugin Output

tcp/0

```
  - Installed package : login_1:4.8.1-2ubuntu2.1
  - Fixed package     : login_1:4.8.1-2ubuntu2.2
```

## 185568 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-6478-1 advisory.

- In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines. (CVE-2023-46316)

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

### See Also

https://ubuntu.com/security/notices/USN-6478-1

### Solution

Update the affected traceroute package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

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

## References

| | |
|---|---|
| CVE | CVE-2023-46316 |
| XREF | USN:6478-1 |

## Plugin Information

Published: 2023/11/14, Modified: 2024/01/23

## Plugin Output

tcp/0

```
  - Installed package : traceroute_1:2.1.0-2
  - Fixed package     : traceroute_1:2.1.0-2ubuntu0.22.04.1~esm1


NOTE: The fixed ESM package referenced in this plugin requires a
subscription to Ubuntu Pro to enable the ESM repositories.
```

## 205227 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6950-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6950-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM32 architecture;

- ARM64 architecture;

- Block layer subsystem;

- Bluetooth drivers;

- Clock framework and drivers;

- FireWire subsystem;

- GPU drivers;

- InfiniBand drivers;

- Multiple devices driver;

- EEPROM drivers;

- Network drivers;

- Pin controllers subsystem;

- Remote Processor subsystem;

- S/390 drivers;

- SCSI drivers;

- 9P distributed file system;

- Network file system client;

- SMB network file system;

- Socket messages infrastructure;

- Dynamic debug library;

- Bluetooth subsystem;

- Networking core;

- IPv4 networking;

- IPv6 networking;

- Multipath TCP;

- NSH protocol;

- Phonet protocol;

- TIPC protocol;

- Wireless networking;

- Key management;

- ALSA framework;

- HD-audio driver; (CVE-2024-36883, CVE-2024-36940, CVE-2024-36902, CVE-2024-36975, CVE-2024-36964, CVE-2024-36938, CVE-2024-36931, CVE-2024-35848, CVE-2024-26900, CVE-2024-36967, CVE-2024-36904, CVE-2024-27398, CVE-2024-36031, CVE-2023-52585, CVE-2024-36886, CVE-2024-36937, CVE-2024-36954, CVE-2024-36916, CVE-2024-36905, CVE-2024-36959, CVE-2024-26980, CVE-2024-26936, CVE-2024-36928, CVE-2024-36889, CVE-2024-36929, CVE-2024-36933, CVE-2024-27399, CVE-2024-36946, CVE-2024-36906, CVE-2024-36965, CVE-2024-36957, CVE-2024-36941, CVE-2024-36897, CVE-2024-36952, CVE-2024-36947, CVE-2024-36950, CVE-2024-36880, CVE-2024-36017, CVE-2023-52882, CVE-2024-36969, CVE-2024-38600, CVE-2024-36955, CVE-2024-36960, CVE-2024-27401, CVE-2024-36919, CVE-2024-36934, CVE-2024-35947, CVE-2024-36953, CVE-2024-36944, CVE-2024-36939)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6950-1

## Solution

Update the affected kernel package.

## Risk Factor

Medium

## CVSS v3.0 Base Score

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

## CVSS v3.0 Temporal Score

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

## VPR Score

7.4

EPSS Score

0.0005

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-52585 |
| CVE | CVE-2023-52882 |
| CVE | CVE-2024-26900 |
| CVE | CVE-2024-26936 |
| CVE | CVE-2024-26980 |
| CVE | CVE-2024-27398 |
| CVE | CVE-2024-27399 |
| CVE | CVE-2024-27401 |
| CVE | CVE-2024-35848 |
| CVE | CVE-2024-35947 |
| CVE | CVE-2024-36017 |
| CVE | CVE-2024-36031 |
| CVE | CVE-2024-36880 |
| CVE | CVE-2024-36883 |
| CVE | CVE-2024-36886 |
| CVE | CVE-2024-36889 |
| CVE | CVE-2024-36897 |
| CVE | CVE-2024-36902 |
| CVE | CVE-2024-36904 |
| CVE | CVE-2024-36905 |
| CVE | CVE-2024-36906 |
| CVE | CVE-2024-36916 |
| CVE | CVE-2024-36919 |
| CVE | CVE-2024-36928 |
| CVE | CVE-2024-36929 |
| CVE | CVE-2024-36931 |
| CVE | CVE-2024-36933 |
| CVE | CVE-2024-36934 |
| CVE | CVE-2024-36937 |

| | |
|---|---|
| CVE | CVE-2024-36938 |
| CVE | CVE-2024-36939 |
| CVE | CVE-2024-36940 |
| CVE | CVE-2024-36941 |
| CVE | CVE-2024-36944 |
| CVE | CVE-2024-36946 |
| CVE | CVE-2024-36947 |
| CVE | CVE-2024-36950 |
| CVE | CVE-2024-36952 |
| CVE | CVE-2024-36953 |
| CVE | CVE-2024-36954 |
| CVE | CVE-2024-36955 |
| CVE | CVE-2024-36957 |
| CVE | CVE-2024-36959 |
| CVE | CVE-2024-36960 |
| CVE | CVE-2024-36964 |
| CVE | CVE-2024-36965 |
| CVE | CVE-2024-36967 |
| CVE | CVE-2024-36969 |
| CVE | CVE-2024-36975 |
| CVE | CVE-2024-38600 |
| XREF | USN:6950-1 |

## Plugin Information

Published: 2024/08/08, Modified: 2024/08/08

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-116-generic does not meet the minimum fixed level of 5.15.0-118-
generic for this advisory.
```

## 10114 - ICMP Timestamp Request Remote Date Disclosure

### Synopsis

It is possible to determine the exact time set on the remote host.

### Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

### Solution

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

### Risk Factor

Low

### VPR Score

4.2

### EPSS Score

0.8808

### CVSS v2.0 Base Score

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

### References

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

### Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

### Plugin Output

icmp/0

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

## 156000 - Apache Log4j Installed (Linux / Unix)

### Synopsis

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

### Description

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

The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' scanner setting in Nessus 8.15.1 or later.

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

### See Also

https://logging.apache.org/log4j/2.x/

### Solution

n/a

### Risk Factor

None

### References

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

### Plugin Information

Published: 2021/12/10, Modified: 2024/08/08

### Plugin Output

tcp/0

```
  Path                           : /usr/share/java/libintl-0.21.jar
  Version                        : unknown
  JMSAppender.class association  : Not Found
  JdbcAppender.class association : Not Found
  JndiLookup.class association   : Not Found
  Method                         : Embedded string inspection


Note: Jar file inspection cannot be performed.  No results or cannot list archive contents.  If
 results are present, install an unzip package to resolve this problem.
```

## 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      : 2.2
Vendor       : American Megatrends Inc.
Release Date : 05/23/2018
UUID         : 00000000-0000-0000-0000-ac1f6b7511f4
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: 2024/07/31

### Plugin Output

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:22.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:log4j -> Apache Software Foundation log4j
  cpe:/a:docker:docker:27.1.1 -> Docker
  cpe:/a:gnupg:libgcrypt:1.8.8 -> GnuPG Libgcrypt
  cpe:/a:gnupg:libgcrypt:1.9.4 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.81.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.81.0 -> Haxx libcurl
  cpe:/a:openbsd:openssh:8.9 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:8.9p1 -> OpenBSD OpenSSH
  cpe:/a:openssl:openssl:1.1.1k -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.1.1w -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:3.0.2 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:3.1.3 -> OpenSSL Project OpenSSL
```

```
    cpe:/a:sqlite:sqlite -> SQLite
    cpe:/a:tukaani:xz -> Tukaani XZ
    cpe:/a:tukaani:xz:5.2.5 -> Tukaani XZ
    cpe:/a:tukaani:xz:5.4.3 -> Tukaani XZ
    cpe:/a:vim:vim:8.2 -> 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: 2024/08/08

### Plugin Output

tcp/0

```
Path               : /usr/bin/curl
Version            : 7.81.0
Associated Package : curl 7.81.0-1ubuntu1.16
Managed by OS      : True
```

## 132634 - Deprecated SSLv2 Connection Attempts

### Synopsis

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

### Description

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

### Solution

N/A

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

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

Plugin ID: 42476
Timestamp: 2024-08-12 11:49:59
Port: 22
```

## 55472 - Device Hostname

### Synopsis

It was possible to determine the remote system hostname.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/06/30, Modified: 2024/08/06

### Plugin Output

tcp/0

```
Hostname : s01-chzrh1-arma
  s01-chzrh1-arma (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 : 100
```

## 111529 - Docker Container Number of Changed Files

### Synopsis

Checks for changes in running Docker containers and reports how many files changed.

### Description

This plugin checks the docker diff information for each container and reports the number of changed files.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/08/03, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Docker container 39a784bc9db35e425671bd4d58671ec61d1a6b28c5a3291544e2d9203df714a5 has 7 changed
 files

Docker container a341ef4c5ecd0d0f8267b03b7589ef357de7ce4f3965bec9ebe2ec39fcc7b89b has 3 changed
 files

Docker container fd1e2918b0f80af8a2a7c9608bed598f8315baeec069f51d83ea5b56ea14dd09 has 6 changed
 files

Docker container b722755a4d5d5fdea0a1b483e688689e1a2372690c147ee9f132ca5fdeadc78f has 18 changed
 files

Docker container d2e8c22f146fd1acc4eddc3503548cd7c1fded27ead60b627e7da28d094be11d has 14 changed
 files

Docker container 25275e453ba0df8badbeb0c06dbd1f7369b3082c92325acb4afcdc05ae704528 has 26 changed
 files

Docker container 460cd338334bb6ca693e8c1f60b45db1d2b3b6a067aedbc955dcb2f2991d5574 has 9 changed
 files

Docker container e785c1aa0945f3c81683fc118cbf4a27dd82cba2cce29ec747afabf22c5c3f89 has 6 changed
 files
```

```
Docker container 9c5dddbf7e4614bef6f7c7517ec165898d85a609789436f213fc5d8321920fc9 has 6 changed
 files

Docker container 3ae6746f30fe1e6171c8bc483fb786333c94defabb727cdbb7393896aa80abb2 has 6 changed
 files

Docker container c9c2de4a24690a85237d1a09330dc87ecdc7fbcdae521f1e2a0ed9793f7026e6 has 5 changed
 files
```

## 159488 - Docker Installed (Linux)

### Synopsis

Docker was detected on the remote host.

### Description

A container virtualization suite is installed on the remote host.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/04, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Path    : /usr/bin/docker
Version : 27.1.1
build   : 6312585
```

## 93561 - Docker Service Detection

### Synopsis

Docker was detected on the remote host.

### Description

The Docker service is running on the remote host. Docker is an open-source project that automates the deployment of applications inside software containers.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/09/16, Modified: 2024/08/08

### Plugin Output

tcp/0

```
  Version: 27.1.1
  Version: 27.1.1
  Version: 1.7.19
  Version: 1.7.19
  Version: 0.19.0

The following containers were detected running on the remote Docker host :

Name:      /dataplane-control
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        39a784bc9db35e425671bd4d58671ec61d1a6b28c5a3291544e2d9203df714a5
Ports:     n/a

Name:      /telemetry
Image:     opentelemetry-collector
Image ID : sha256:1664fef5e8077e3c42f917dacd7aba8b339d6c9925cd5c9d6d7cee2e0d1d4ce7
Tag:       v0.36.3
ID:        a341ef4c5ecd0d0f8267b03b7589ef357de7ce4f3965bec9ebe2ec39fcc7b89b
Ports:     n/a

Name:      /gateway
Image:     scion-all
```

```
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        fd1e2918b0f80af8a2a7c9608bed598f8315baeec069f51d83ea5b56ea14dd09
Ports:     n/a

Name:      /dataplane
Image:     vpp-dataplane
Image ID : sha256:c30fa9fd28754cc2328e51f64f4b05aa56aee255f98d5b6c4b3952b75e22f50d
Tag:       v0.36.3
ID:        b722755a4d5d5fdea0a1b483e688689e1a2372690c147ee9f132ca5fdeadc78f
Ports:     n/a

Name:      /daemon-64-2_0_2b
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        d2e8c22f146fd1acc4eddc3503548cd7c1fded27ead60b627e7da28d094be11d
Ports:     n/a

Name:      /control-64-2_0_2b
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        25275e453ba0df8badbeb0c06dbd1f7369b3082c92325acb4afcdc05ae704528
Ports:     n/a

Name:      /appliance-cron
Image:     appliance
Image ID : sha256:e10607406bb6806690db889fdf91e7332bf652d15529798846c46244de03d2eb
Tag:       v0.36.3
ID:        460cd338334bb6ca693e8c1f60b45db1d2b3b6a067aedbc955dcb2f2991d5574
Ports:     n/a

Name:      /router
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        e785c1aa0945f3c8168 [...]
```

## 25203 - Enumerate IPv4 Interfaces via SSH

### Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

### Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

### Solution

Disable any unused IPv4 interfaces.

### Risk Factor

None

### Plugin Information

Published: 2007/05/11, Modified: 2024/02/05

### Plugin Output

tcp/0

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

 - 172.17.0.1 (on interface docker0)
 - 192.168.130.20 (on interface eno1)
 - 192.168.111.1 (on interface enp2s0f1)
 - 127.0.0.1 (on interface lo)
 - 198.18.30.2 (on interface wg0)
```

## 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 :

 - fe80::ae1f:6bff:fe75:11f4 (on interface eno1)
 - fe80::2:0:2b:1 (on interface enp2s0f0)
 - fe80::21b:21ff:febe:3452 (on interface enp2s0f1)
 - ::1 (on interface lo)
 - fe80::7b81:8132:be2e:1973 (on interface scion-gateway)
```

## 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 :

  - 02:42:7a:09:6d:69 (interface docker0)
  - ac:1f:6b:75:11:f5 (interface eno2)
  - 00:1b:21:be:34:50 (interface enp2s0f0)
  - 00:1b:21:be:34:52 (interface enp2s0f1)
  - ac:1f:6b:75:11:f4 (interface eno1)
```

## 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

```
enp2s0f1:
  MAC : 00:1b:21:be:34:52
  IPv4:
    - Address : 192.168.111.1
      Netmask : 255.255.255.0
      Broadcast : 192.168.111.255
  IPv6:
    - Address : fe80::21b:21ff:febe:3452
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
eno1:
  MAC : ac:1f:6b:75:11:f4
  IPv4:
    - Address : 192.168.130.20
      Netmask : 255.255.255.0
      Broadcast : 192.168.130.255
  IPv6:
    - Address : fe80::ae1f:6bff:fe75:11f4
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
enp2s0f0:
  MAC : 00:1b:21:be:34:50
  IPv6:
    - Address : fe80::2:0:2b:1
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
wg0:
  IPv4:
    - Address : 198.18.30.2
```

```
        Netmask : 255.255.255.255
docker0:
  MAC : 02:42:7a:09:6d:69
  IPv4:
    - Address : 172.17.0.1
        Netmask : 255.255.0.0
        Broadcast : 172.17.255.255
eno2:
  MAC : ac:1f:6b:75:11:f5
lo:
  IPv4:
    - Address : 127.0.0.1
        Netmask : 255.0.0.0
  IPv6:
    - Address : ::1
        Prefixlen : 128
        Scope : host
        ScopeID : 0x10
scion-gateway:
  IPv6:
    - Address : fe80::7b81:8132:be2e:1973
        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:
  wg0:
    ipv4_gateways:
      198.18.0.1:
        subnets:
          - 198.18.0.0/24
Interface Routes:
  docker0:
    ipv4_subnets:
      - 172.17.0.0/16
  eno1:
    ipv4_subnets:
      - 192.168.130.0/24
    ipv6_subnets:
      - fe80::/64
  enp2s0f0:
    ipv6_subnets:
      - fe80::/64
  enp2s0f1:
    ipv4_subnets:
      - 192.168.111.0/24
    ipv6_subnets:
      - fe80::/64
  scion-gateway:
    ipv4_subnets:
      - 0.0.0.0/1
      - 128.0.0.0/2
      - 192.0.0.0/9
      - 192.128.0.0/11
      - 192.160.0.0/13
      - 192.168.0.0/18
      - 192.168.64.0/19
```

```
      - 192.168.96.0/21
      - 192.168.104.0/22
      - 192.168.108.0/23
      - 192.168.110.0/24
      - 192.168.111.0/24
      - 192.168.112.0/24
      - 192.168.113.0/24
      - 192.168.114.0/23
      - 192.168.116.0/22
      - 192.168.120.0/21
      - 192.168.128.0/21
      - 192.168.136.0/22
      - 192.168.141.0/24
      - 192.168.142.0/23
      - 192.168.144.0/20
      - 192.168.160.0/19
      - 192.168.192.0/18
      - 192.169.0.0/16
      - 192.170.0.0/15
      - 192.172.0.0/14
      - 192.176.0.0/12
      - 192.192.0.0/10
      - 193.0.0.0/8
      - 194.0.0.0/7
      - 196.0.0.0/6
      - 200.0.0.0/5
      - 208.0.0.0/4
      - 224.0.0.0/3
    ipv6_subnets:
      - fe80::/64
```

## 168980 - Enumerate the PATH Variables

### Synopsis

Enumerates the PATH variable of the current scan user.

### Description

Enumerates the PATH variables of the current scan user.

### Solution

Ensure that directories listed here are in line with corporate policy.

### Risk Factor

None

### Plugin Information

Published: 2022/12/21, Modified: 2024/08/08

### 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
/snap/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 :

AC:1F:6B:75:11:F5 : Super Micro Computer, Inc.
00:1B:21:BE:34:50 : Intel Corporate
00:1B:21:BE:34:52 : Intel Corporate
AC:1F:6B:75:11:F4 : Super Micro Computer, 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:
  - 02:42:7A:09:6D:69
  - AC:1F:6B:75:11:F5
  - 00:1B:21:BE:34:50
  - 00:1B:21:BE:34:52
  - AC:1F:6B:75:11:F4
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/443/www

```
1 external URL was gathered on this web server :
URL...                                  - Seen on...


https://fonts.gstatic.com               - /ui
```

## 84502 - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

https://tools.ietf.org/html/rfc6797

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
HTTP/1.1 301 Moved Permanently
Alt-Svc: h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000
Content-Length: 38
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Aug 2024 11:50:24 GMT
Location: /ui
Server: Caddy
Connection: close

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

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

```
Based on tests of each method :

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

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Based on tests of each method :

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

    /
    /ui
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

```
Based on tests of each method :

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

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

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

### Plugin Output

tcp/80/www

```
The remote web server type is :

Caddy
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The remote web server type is :

Caddy
```

## 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/42001/www

```
The remote web server type is :

Caddy
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 308 Permanent Redirect

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

  Connection: close
  Location: https://192.168.111.1/
  Server: Caddy
  Date: Mon, 12 Aug 2024 11:56:52 GMT
  Content-Length: 0

Response Body :
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 301 Moved Permanently

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

  Alt-Svc: h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000
  Content-Length: 38
  Content-Type: text/html; charset=utf-8
  Date: Mon, 12 Aug 2024 11:56:52 GMT
  Location: /ui
  Server: Caddy
  Connection: close

Response Body :

<a href="/ui">Moved Permanently</a>.
```

## 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/42001/www

```
Response Code : HTTP/1.1 200 OK

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

  Server: Caddy
  Date: Mon, 12 Aug 2024 11:56:52 GMT
  Content-Length: 0
  Connection: close

Response Body :
```

## 91634 - HyperText Transfer Protocol (HTTP) Redirect Information

### Synopsis

The remote web server redirects requests to the root directory.

### Description

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

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

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Request         : https://192.168.111.1/
HTTP response   : HTTP/1.1 301 Moved Permanently
Redirect to     : https://192.168.111.1/ui
Redirect type   : 30x redirect

Final page      : https://192.168.111.1/ui
HTTP response   : HTTP/1.1 200 OK
```

## 171410 - IP Assignment Method Detection

### Synopsis

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

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/02/14, Modified: 2024/08/08

### Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ eno1
  + IPv4
    - Address       : 192.168.130.20
      Assign Method : static
  + IPv6
    - Address       : fe80::ae1f:6bff:fe75:11f4
      Assign Method : static
+ eno2
+ wg0
  + IPv4
    - Address       : 198.18.30.2
      Assign Method : static
+ docker0
  + IPv4
    - Address       : 172.17.0.1
      Assign Method : static
+ enp2s0f0
  + IPv6
    - Address       : fe80::2:0:2b:1
      Assign Method : static
+ enp2s0f1
  + IPv4
    - Address       : 192.168.111.1
      Assign Method : static
  + IPv6
```

```
    - Address       : fe80::21b:21ff:febe:3452
      Assign Method : static
+ scion-gateway
  + IPv6
    - Address       : fe80::7b81:8132:be2e:1973
      Assign Method : static
+ i.ABAAAAQAAAACW
```

## 14788 - IP Protocols Scan

### Synopsis

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

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
4IP
6TCP
17UDP
41IPv6
50ESP
103PIM
112VRRP
136UDPLite
```

## 118237 - JAR File Detection for Linux/UNIX

### Synopsis

Detected JAR files on the host.

### Description

The host contains JAR files, Java Archive files.

Note that this plugin only detects JAR files in commonly used installation directories or a user specified search path.

### See Also

https://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/22, Modified: 2024/08/08

### Plugin Output

tcp/0

```
JAR files found: 1
 - /usr/share/java/libintl-0.21.jar
```

## 151883 - Libgcrypt Installed (Linux/UNIX)

### Synopsis

Libgcrypt is installed on this host.

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/07/21, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 14 installs of Libgcrypt:

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/usr/lib/x86_64-linux-
gnu/libgcrypt.so.20.2.8
  Version : 1.8.8
```

```
  Path    : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/usr/lib/x86_64-linux-
gnu/libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/TDWKMHQV2KHBJAL4KZXBAD3QKJ/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/TDWKMHQV2KHBJAL4KZXBAD3QKJ/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/ULEKMISDKAANXMLQQS5EGTXAXE/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/ULEKMISDKAANXMLQQS5EGTXAXE/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.8
  Version : 1.8.8
```

## 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
tmpfs                              6.3G  2.2M  6.3G   1% /run
/dev/mapper/anapaya--v3--vg-root   229G   23G  196G  11% /
tmpfs                               32G     0   32G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
overlay                            229G   23G  196G  11% /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged
overlay                            229G   23G  196G  11% /var/lib/docker/
overlay2/0484dd6393932f0dd5948c7176dca65d6c46fbcfe59898ad478659e3cffec6c0/merged
overlay                            229G   23G  196G  11% /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged
overlay                            229G   23G  196G  11% /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged
overlay                            229G   23G  196G  11% /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged
overlay                            229G   23G  196G  11% /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged
overlay                            229G   23G  196G  11% /var/lib/docker/
overlay2/15489e211324425911aeb0bcde8bce23178d14aac0fa62fd916b46d59e8a672b/merged
overlay                            229G   23G  196G  11% /var/lib/docker/
overlay2/266c7e799edd66418fcdd01f1f4bbdb28c7444bd588701b621754120433f66e5/merged
overlay                            229G   23G  196G  11% /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged
```

```
overlay                          229G   23G  196G  11% /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged
overlay                          229G   23G  196G  11% /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged


$ lsblk
NAME                      MAJ: [...]
```

## 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: Etc/UTC (UTC, +0000)
Via /etc/timezone: Etc/UTC
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: 2024/03/13

### Plugin Output

tcp/0

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

User         : anapaya
Home folder  : /home/anapaya
Start script : /bin/bash
Groups       : anapaya
               dip
               lpadmin
               wireshark
               cdrom
               adm
               sudo
               sambashare
               plugdev

User         : scion
Home folder  : /home/scion
Start script : /bin/bash
Groups       : scion
               sudo
               adm

User         : prometheus
Home folder  : /
Start script : /bin/false
Groups       : prometheus

User         : william.blonay
Home folder  : /home/william.blonay
```

```
Start script : /bin/bash
Groups       : sudo
               william.blonay

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

User         : root
Home folder  : /root
Start script : /bin/bash
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   : /v [...]
```

## 45433 - Memory Information (via DMI)

### Synopsis

Information about the remote system's memory devices can be read.

### Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/06, Modified: 2018/03/29

### Plugin Output

tcp/0

```
Total memory : 65536 MB
```

## 50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

### See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

### Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/443/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - https://192.168.111.1/ui
  - https://192.168.111.1/ui/
```

## 50345 - Missing or Permissive X-Frame-Options HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

### See Also

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

http://www.nessus.org/u?399b1f56

### Solution

Set a properly configured X-Frame-Options header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/443/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - https://192.168.111.1/ui
  - https://192.168.111.1/ui/
```

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/08/05

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.1
Nessus build : 20004
Plugin feed version : 202408120709
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Advanced Scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.110.80
Port scanner(s) : netstat
Port range : 0-65535
Ping RTT : 90.118 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'anapaya' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : never
Max hosts : 100
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 : 2024/8/12 13:48 CEST
Scan duration : 1376 sec
Scan for malware : yes
```

## 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: 2024/07/24

### 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: 2024/07/24

### Plugin Output

tcp/80/www

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

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

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

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

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/07/24

### Plugin Output

tcp/443/www

```
Port 443/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: 2024/07/24

### Plugin Output

udp/443

```
Port 443/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: 2024/07/24

### Plugin Output

udp/30041

```
Port 30041/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: 2024/07/24

### Plugin Output

udp/30042

```
Port 30042/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: 2024/07/24

### Plugin Output

tcp/30252

```
Port 30252/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: 2024/07/24

### Plugin Output

tcp/42001/www

```
Port 42001/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: 2024/07/24

### Plugin Output

udp/51021

```
Port 51021/udp was found to be open
```

## 33851 - Network daemons not managed by the package system

### Synopsis

Some daemon processes on the remote host are associated with programs that have been installed manually.

### Description

Some daemon processes on the remote host are associated with programs that have been installed manually.

System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

### Solution

Use packages supplied by the operating system vendor whenever possible.

And make sure that manual software installation agrees with your organization's acceptable use and security policies.

### Risk Factor

None

### Plugin Information

Published: 2008/08/08, Modified: 2024/03/06

### Plugin Output

tcp/0

```
The following running daemons are not managed by dpkg :

/usr/local/bin/appliance
/usr/local/bin/debugscraper
```

## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/12/09, Modified: 2024/06/19

### Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 5.15.0-116-generic on Ubuntu 22.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 5.15.0-116-generic on Ubuntu 22.04
```

## 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: 2024/03/19

### Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'publickey' authentication.

The output of "uname -a" is :
Linux s01-chzrh1-arma 5.15.0-116-generic #126-Ubuntu SMP Mon Jul 1 10:14:24 UTC 2024 x86_64 x86_64
 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
bookworm/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 30.141 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.

Account  : anapaya
Protocol : SSH
```

## 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: 2024/08/08

### Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.9p1
Banner  : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
```

## 168007 - OpenSSL Installed (Linux)

### Synopsis

OpenSSL was detected on the remote Linux host.

### Description

OpenSSL was detected on the remote Linux host.

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

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

### See Also

https://openssl.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/11/21, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 42 installs of OpenSSL:

  Path    : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
cbb391c3bbc1d14a56fc7d63b1e49c07c8a075b6a0988db8e216ff1974191bcf/diff/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Version : 1.1.1k
```

```
  Path    : /var/lib/docker/overlay2/
b86bd05b8bb9de05816892b7f36d07cb5504de897fc3147ac7b2cd22a2404a2e/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/5c593833ee4882835dc9f36f8a460cdade54dd52311ae1162d2501dd72377f77/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/3b1d277dc0611d125e6edd3323ac9954a14614abaaeb11b2172a3aa94f1db284/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/3142c7f346756b583afeb33378aff933af1e22148ba72a46ebb573bc4d897355/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/359e3c8fc308757ce4b2d7cc7a60c6a952092522fba9859061c33ce9a51cc175/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/9fc980a0845edd0dfcec3da9c08ab733a619f5b10f736f2ae4671b1931286db5/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/usr/bin/openssl
  Version : 1.1.1w

  Path    : /var/lib/docker/
overlay2/1a76dcd30f60c22fe5111760cfbbd44ab2c1050fda33256282e749cd48a48759/diff/lib/libcrypto.so.3
  Version : 3.1.3

  Path    : /var/lib/docker/
overlay2/5025ed8860b45e319a4fc94cf98dc606c32142df5cbddfab164772fffc68cf2b/merged/usr/lib/x8 [...]
```

## 66334 - Patch Report

### Synopsis

The remote host is missing several patches.

### Description

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

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

### Solution

Install the patches listed below.

### Risk Factor

None

### Plugin Information

Published: 2013/07/08, Modified: 2024/07/15

### Plugin Output

tcp/0

```
. You need to take the following 14 actions :

[ OpenSSL 1.1.1 < 1.1.1za Vulnerability (201084) ]

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

[ OpenSSL 3.0.0 < 3.0.15 Vulnerability (201085) ]

+ Action to take : Upgrade to OpenSSL version 3.0.15 or later.

+Impact : Taking this action will resolve 40 different vulnerabilities (CVEs).

[ OpenSSL 3.1.0 < 3.1.7 Vulnerability (201082) ]

+ Action to take : Upgrade to OpenSSL version 3.1.7 or later.

[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability
 (USN-6640-1) (190598) ]

+ Action to take : Update the affected packages.
```

```
[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos
 vulnerabilities (USN-6947-1) (205195) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)
 (185568) ]

+ Action to take : Update the affected traceroute package.


[ Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : pip vulnerabilities
 (USN-6473-2) (185739) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1) (195216) ]

+ Action to take : Update the affected packages.


[ Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenSSL vulnerabilities (USN-6937-1) (204924) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-6944-1) (204989) ]

+ Action to take : Update the affected packages.


[ Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6923-1) (204913) ]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnera [...]
```

## 45432 - Processor Information (via DMI)

### Synopsis

Nessus was able to read information about the remote system's processor.

### Description

Nessus was able to retrieve information about the remote system's hardware, such as its processor type, by using the SMBIOS (aka DMI) interface.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/06, Modified: 2016/02/25

### Plugin Output

tcp/0

```
Nessus detected 1 processor :

Current Speed   : 3800 MHz
Version         : Intel(R) Xeon(R) CPU E3-1275 v6 @ 3.80GHz
Manufacturer    : Samsung
External Clock  : 100 MHz
Status          : Valid, Not Full
Family          : Xeon
Type            : DDR4
```

## 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   : 12772
Executable   : /usr/sbin/sshd
Command line : sshd: /usr/sbin/sshd -D [listener] 1 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

tcp/80/www

```
Process ID   : 187660
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 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/443/www

```
Process ID   : 187660
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 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/443

```
Process ID   : 187660
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 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/30041

```
Process ID   : 195372
Executable   : /app/scion-all
Command line : /app/scion-all dispatcher --config /share/conf/dispatcher.toml
```

## 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/30042

```
Process ID   : 195788
Executable   : /usr/bin/vpp
Command line : /usr/bin/vpp -c /share/conf/dataplane.conf
```

## 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/30252

```
Process ID   : 195497
Executable   : /app/scion-all
Command line : /app/scion-all control --config /share/conf/control.toml
```

## 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/42001/www

```
Process ID   : 187660
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 174788 - SQLite Local Detection (Linux)

### Synopsis

The remote Linux host has SQLite Database software installed.

### Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

### See Also

https://www.sqlite.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/04/26, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Path    : /usr/share/bash-completion/completions/sqlite3
Version : unknown
```

## 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: 2017/08/28

### Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

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

The server supports the following options for server_host_key_algorithms :

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

The server supports the following options for encryption_algorithms_client_to_server :

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

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

The server supports the following options for encryption_algorithms_server_to_client :

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

The server supports the following options for mac_algorithms_client_to_server :

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

The server supports the following options for mac_algorithms_server_to_client :

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

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@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
```

## 90707 - SSH SCP Protocol Detection

### Synopsis

The remote host supports the SCP protocol over SSH.

### Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

### Plugin Output

tcp/22/ssh

## 153588 - SSH SHA-1 HMAC Algorithms Enabled

### Synopsis

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

### Description

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

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/22/ssh

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

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

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

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

## 10267 - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

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

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0933

### Plugin Information

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

### Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
SSH supported authentication : publickey
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

### Plugin Output

tcp/443/www

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

## 83298 - SSL Certificate Chain Contains Certificates Expiring Soon

### Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

### Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

### Solution

Renew any soon to expire SSL certificates.

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

|-Subject   : CN=Caddy Local Authority - ECC Intermediate
|-Not After : Aug 14 15:32:17 2024 GMT

|-Subject   :
|-Not After : Aug 12 23:18:58 2024 GMT
```

## 42981 - SSL Certificate Expiry - Future Expiry

### Synopsis

The SSL certificate associated with the remote service will expire soon.

### Description

The SSL certificate associated with the remote service will expire soon.

### Solution

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

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
The SSL certificate will expire within 60 days, at
Aug 12 23:18:58 2024 GMT :

  Subject          : n/a
  Issuer           : CN=Caddy Local Authority - ECC Intermediate
  Not valid before : Aug 12 11:18:58 2024 GMT
  Not valid after  : Aug 12 23:18:58 2024 GMT
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 00 AF 71 BE 4F 53 49 D7 91 43 E7 A5 EF 6A B5 CC CC

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:18:58 2024 GMT
Not Valid After: Aug 12 23:18:58 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 82 F5 DB 1D DD D0 57 C5 D9 69 02 51 3F 35 7D CE DE C1 5D 3D
              4F 5E 4D 07 C4 4E 61 59 AD 7E 4D 32
Public Key Y: AA C7 82 4C 83 D7 D7 6F 36 6D 51 81 C2 B9 DB 82 BE 6C 3E C3
              B8 D5 BB 58 FB B1 10 22 BC 0F 4B C2

Signature Length: 70 bytes / 560 bits
Signature: 00 30 44 02 20 71 B9 CD C0 C9 2C 35 AB 0F 49 4A 27 D2 3A DC
           78 F5 94 EF 04 C8 A4 1F F6 E6 E9 FF 45 9D D2 65 7E 02 20 1D
           F2 68 64 A9 D7 97 F8 BE 82 59 D6 4E A7 F0 11 82 7A B8 10 0A
           60 D6 50 CF F9 31 B2 D8 77 B3 5B
```

```
Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CF 71 74 4F E7 D3 2A 7F DC 43 C7 28 F4 1C 95 0D FC 35 59 CD


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 1F 42 4B DA E2 E5 00 B1 32 56 D3 CE F3 AD F1 EF 34 FA 4A A7


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1


Fingerprints :

SHA-256 Fingerprint: FA 28 C0 87 50 43 FD 25 BC 4A C5 64 00 07 F9 51 D2 FF AA B4
                     18 88 A7 FE DA 16 A5 8D 98 91 46 47
SHA-1 Fingerprint: F7 2A 46 C9 E4 0C E6 05 BA 56 51 FF E4 83 32 EB 47 63 9C B6
MD5 Fingerprint: 8C 4D D9 E3 ED 65 B0 3A 36 34 CB 06 AF 86 39 A8


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuDCCAV+gAwIBAgIRAK9xvk9TSdeRQ
+el72q1zMwwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA4MTIxMTE
 [...]
```

## 159544 - SSL Certificate with no Common Name

### Synopsis

Checks for an SSL certificate with no Common Name

### Description

The remote system is providing an SSL/TLS certificate without a subject common name field. While this is not required in all cases, it is recommended to ensure broad compatibility.

### See Also

https://datatracker.ietf.org/doc/html/rfc5280#section-4.1.2.6

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/06, Modified: 2022/11/30

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 00 AF 71 BE 4F 53 49 D7 91 43 E7 A5 EF 6A B5 CC CC

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:18:58 2024 GMT
Not Valid After: Aug 12 23:18:58 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 82 F5 DB 1D DD D0 57 C5 D9 69 02 51 3F 35 7D CE DE C1 5D 3D
              4F 5E 4D 07 C4 4E 61 59 AD 7E 4D 32
Public Key Y: AA C7 82 4C 83 D7 D7 6F 36 6D 51 81 C2 B9 DB 82 BE 6C 3E C3
```

```
              B8 D5 BB 58 FB B1 10 22 BC 0F 4B C2

Signature Length: 70 bytes / 560 bits
Signature: 00 30 44 02 20 71 B9 CD C0 C9 2C 35 AB 0F 49 4A 27 D2 3A DC
           78 F5 94 EF 04 C8 A4 1F F6 E6 E9 FF 45 9D D2 65 7E 02 20 1D
           F2 68 64 A9 D7 97 F8 BE 82 59 D6 4E A7 F0 11 82 7A B8 10 0A
           60 D6 50 CF F9 31 B2 D8 77 B3 5B

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CF 71 74 4F E7 D3 2A 7F DC 43 C7 28 F4 1C 95 0D FC 35 59 CD


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 1F 42 4B DA E2 E5 00 B1 32 56 D3 CE F3 AD F1 EF 34 FA 4A A7


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuDCCAV+gAwIBAgIRAK9xvk9TSdeRQ
+el72q1zMwwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA4MTIxMTE
NX3O3sFdPU9eTQfETmFZrX5NMqrHgkyD19dvNm1RgcK524K+bD7DuNW7WPuxECK8D0vCo4GGMIGDMA4GA1UdDwEB/
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFM9xdE/
n0yp/3EPHKPQclQ38NVnNMB8GA1UdIwQYMBaAFB9CS9ri5QCxMlbTzvOt8e80+kqnMBIGA1UdEQEB/wQIMAaHBMC [...]
```

## 159545 - SSL Certificate with no Subject

### Synopsis

Checks for an SSL certificate with no Subject

### Description

The remote system is providing an SSL/TLS certificate without a subject field. While this is not required in all cases, it is recommended to ensure broad compatibility.

### See Also

https://datatracker.ietf.org/doc/html/rfc5280#section-4.1.2.6

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/06, Modified: 2022/11/30

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 00 AF 71 BE 4F 53 49 D7 91 43 E7 A5 EF 6A B5 CC CC

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:18:58 2024 GMT
Not Valid After: Aug 12 23:18:58 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 82 F5 DB 1D DD D0 57 C5 D9 69 02 51 3F 35 7D CE DE C1 5D 3D
              4F 5E 4D 07 C4 4E 61 59 AD 7E 4D 32
Public Key Y: AA C7 82 4C 83 D7 D7 6F 36 6D 51 81 C2 B9 DB 82 BE 6C 3E C3
```

```
              B8 D5 BB 58 FB B1 10 22 BC 0F 4B C2

Signature Length: 70 bytes / 560 bits
Signature: 00 30 44 02 20 71 B9 CD C0 C9 2C 35 AB 0F 49 4A 27 D2 3A DC
           78 F5 94 EF 04 C8 A4 1F F6 E6 E9 FF 45 9D D2 65 7E 02 20 1D
           F2 68 64 A9 D7 97 F8 BE 82 59 D6 4E A7 F0 11 82 7A B8 10 0A
           60 D6 50 CF F9 31 B2 D8 77 B3 5B

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CF 71 74 4F E7 D3 2A 7F DC 43 C7 28 F4 1C 95 0D FC 35 59 CD


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 1F 42 4B DA E2 E5 00 B1 32 56 D3 CE F3 AD F1 EF 34 FA 4A A7


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuDCCAV+gAwIBAgIRAK9xvk9TSdeRQ
+el72q1zMwwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA4MTIxMTE
NX3O3sFdPU9eTQfETmFZrX5NMqrHgkyD19dvNm1RgcK524K+bD7DuNW7WPuxECK8D0vCo4GGMIGDMA4GA1UdDwEB/
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFM9xdE/
n0yp/3EPHKPQclQ38NVnNMB8GA1UdIwQYMBaAFB9CS9ri5QCxMlbTzvOt8e80+kqnMBIGA1UdEQEB/wQIMAaHBMC [...]
```

## 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/443/www

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

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


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B        ECDH          ECDSA    AES-GCM(128)
 SHA256
```

```
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C       ECDH           ECDSA    AES-GCM(256)
 SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9       ECDH           ECDSA    ChaCha20-Poly1305(256)
 SHA256

The fields above are :

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

## 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

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

### Description

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

### See Also

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

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B        ECDH          ECDSA    AES-GCM(128)
 SHA256
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C        ECDH          ECDSA    AES-GCM(256)
 SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9        ECDH          ECDSA    ChaCha20-Poly1305(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/22/ssh

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/80/www

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

tcp/443/www

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

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

```
A web server is 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: 2022/09/06

### Plugin Output

tcp/0

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

  ii   adduser  3.118ubuntu5  all  add and remove users and groups
  ii   amd64-microcode  3.20191218.1ubuntu2.2  amd64  Processor microcode firmware for AMD CPUs
  ii   anapaya-appliance-installer  1.3.0  amd64  The installer of the Anapaya appliance.
  ii   anapaya-system-config  1.4.0  amd64  System configuration for Anapaya appliances.
  ii   apparmor  3.0.4-2ubuntu2.3  amd64  user-space parser utility for AppArmor
  ii   apt  2.4.12  amd64  commandline package manager
  ii   apt-transport-https  2.4.12  all  transitional package for https support
  ii   apt-utils  2.4.12  amd64  package management related utility programs
  ii   base-files  12ubuntu4.6  amd64  Debian base system miscellaneous files
  ii   base-passwd  3.5.52build1  amd64  Debian base system master password and group files
  ii   bash  5.1-6ubuntu1.1  amd64  GNU Bourne Again SHell
  ii   bash-completion  1:2.11-5ubuntu1  all  programmable completion for the bash shell
  ii   bind9-dnsutils  1:9.18.28-0ubuntu0.22.04.1  amd64  Clients provided with BIND 9
  ii   bind9-host  1:9.18.28-0ubuntu0.22.04.1  amd64  DNS Lookup Utility
  ii   bind9-libs  1:9.18.28-0ubuntu0.22.04.1  amd64  Shared Libraries used by BIND 9
  ii   binutils  2.38-4ubuntu2.6  amd64  GNU assembler, linker and binary utilities
  ii   binutils-common  2.38-4ubuntu2.6  amd64  Common files for the GNU assembler, linker and
 binary utilities
  ii   binutils-x86-64-linux-gnu  2.38-4ubuntu2.6  amd64  GNU binary utilities, for x86-64-linux-gnu
 target
```

```
  ii   bsdextrautils  2.37.2-4ubuntu3.4  amd64  extra utilities from 4.4BSD-Lite
  ii   bsdutils  1:2.37.2-4ubuntu3.4  amd64  basic utilities from 4.4BSD-Lite
  ii   busybox-initramfs  1:1.30.1-7ubuntu3  amd64  Standalone shell setup for initramfs
  ii   busybox-static  1:1.30.1-7ubuntu3  amd64  Standalone rescue shell with tons of builtin
utilities
  ii   bzip2  1.0.8-5build1  amd64  high-quality block-sorting file compressor - utilities
  ii   ca-certificates  2 [...]
```

## 118225 - Super Micro detection (dmidecode)

### Synopsis

The remote host is a Super Micro system.

### Description

According to the DMI information, the remote host contains hardware manufactured by Super Micro.

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/19, Modified: 2024/08/08

### Plugin Output

tcp/0

## 35351 - System Information Enumeration (via DMI)

### Synopsis

Information about the remote system's hardware can be read.

### Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/01/12, Modified: 2024/07/29

### Plugin Output

tcp/0

```
Chassis Information
  Serial Number : 0123456789
  Version       : 0123456789
  Manufacturer  : Supermicro
  Lock          : Not Present
  Type          : Main Server Chassis

System Information
  Serial Number : 0123456789
  Version       : 0123456789
  Manufacturer  : Supermicro
  Product Name  : Super Server
  Family        : To be filled by O.E.M.
```

## 25220 - TCP/IP Timestamps Supported

### Synopsis

The remote service implements TCP timestamps.

### Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### See Also

http://www.ietf.org/rfc/rfc1323.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/0

## 136318 - TLS Version 1.2 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.2.

### See Also

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

### Solution

N/A

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

## 138330 - TLS Version 1.3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.3.

### See Also

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

### Solution

N/A

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

## 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/22/ssh

```
Nessus was able to log into the remote host with no privilege or access
problems via the following :

User:       'anapaya'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo
```

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

### Synopsis

Valid credentials were provided for an available authentication protocol.

### Description

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

Please note the following :

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/22/ssh

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

User:       'anapaya'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo
```

## 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  5.15.0-116-gener Wed Jul 24 12:44   still running

wtmp begins Wed Jul  3 09:54:48 2024
```

## 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 192.168.110.80 to 192.168.111.1 :
192.168.110.80
192.168.110.1
?
192.168.111.1

Hop Count: 4
```

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/03/29, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 8 installs of XZ Utils:

  Path           : /var/lib/docker/overlay2/
df7e532060889bf4ffe24ab019911f00a435923bf2b8656f14f5ec3f1724c662/merged/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version        : 5.2.5
```

```
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/overlay2/
d2030fff465c57035cabd63f21b90ac58d3585d1a775d0315869aeb782fc9f71/diff/usr/lib/liblzma.so.5.4.3
  Version        : 5.4.3
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/6df805bb2b12e21afa692b1988ff045a4f6bb4b0df6155c3e83a09c4906fd920/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path    : /var/lib/docker/
overlay2/23309494955c4fc69dc5251f118706e7f0fc1c53a138157c79da2405739a8c4a/diff/bin/xz
  Version : unknown

  Path               : /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.5
  Version            : 5.2.5
  Associated Package : liblzma5 5.2.5-2ubuntu1
  Confidence         : High
  Managed by OS      : True
  Version Source     : Package

  Path               : /usr/bin/xz
  Version            : 5.2.5
  Associated Package : xz-utils 5.2.5-2ubuntu1
  Confidence         : High
  Managed by OS      : True
  Version Source     : Package

  Path    : /var/lib/docker/
overlay2/266c7e799edd66418fcdd01f1f4bbdb28c7444bd588701b621754120433f66e5/merged/bin/xz
  Version : unknown
```

## 183197 - Ubuntu 22.04 ESM : iperf3 vulnerability (USN-6431-3)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 22.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6431-3 advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-6431-3

### Solution

Update the affected iperf3, libiperf-dev and / or libiperf0 packages.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | USN:6431-3 |

### Plugin Information

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

### Plugin Output

tcp/0

```
  - Installed package : iperf3_3.9-1+deb11u1build0.22.04.1
  - Fixed package     : iperf3_3.9-1+deb11u1ubuntu0.1~esm1

  - Installed package : libiperf0_3.9-1+deb11u1build0.22.04.1
  - Fixed package     : libiperf0_3.9-1+deb11u1ubuntu0.1~esm1


NOTE: The fixed ESM packages referenced in this plugin requires a
subscription to Ubuntu Pro to enable the ESM repositories.
```

## 198218 - Ubuntu Pro Subscription Detection

### Synopsis

The remote Ubuntu host has an active Ubuntu Pro subscription.

### Description

The remote Ubuntu host has an active Ubuntu Pro subscription.

### See Also

https://documentation.ubuntu.com/pro/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/05/31, Modified: 2024/07/05

### Plugin Output

tcp/0

```
This machine is NOT attached to an Ubuntu Pro subscription. However, it may have previously been
 attached.

The following details were gathered from /var/lib/ubuntu-advantage/status.json:

Binary Path                  : /var/lib/ubuntu-advantage
Binary Version               : 29.4~22.04
```

## 83303 - Unix / Linux - Local Users Information : Passwords Never Expire

### Synopsis

At least one local user has a password that never expires.

### Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

### Solution

Allow or require users to change their passwords regularly.

### Risk Factor

None

### Plugin Information

Published: 2015/05/10, Modified: 2023/11/27

### Plugin Output

tcp/0

```
Nessus found the following unlocked users with passwords that do not expire :
  - root
  - anapaya
  - scion
```

## 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  0.0 167252 12820 ?        Ss   Jul24  44:57 /sbin/init noquiet nosplash nofb
root           2  0.0  0.0      0     0 ?        S    Jul24   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Jul24   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Jul24   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Jul24   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   Jul24   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   Jul24   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   Jul24   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        S    Jul24   0:00 [rcu_tasks_rude_]
root          12  0.0  0.0      0     0 ?        S    Jul24   0:00 [rcu_tasks_trace]
root          13  0.0  0.0      0     0 ?        S    Jul24   0:45 [ksoftirqd/0]
root          14  0.0  0.0      0     0 ?        I    Jul24  16:10 [rcu_sched]
root          15  0.0  0.0      0     0 ?        S    Jul24   0:01 [migration/0]
root          16  0.0  0.0      0     0 ?        S    Jul24   0:00 [idle_inject/0]
root          18  0.0  0.0      0     0 ?        S    Jul24   0:00 [cpuhp/0]
root          19  0.0  0.0      0     0 ?        S    Jul24   0:00 [cpuhp/1]
root          20  0.0  0.0      0     0 ?        S    Jul24   0:00 [idle_inject/1]
root          21  0.0  0.0      0     0 ?        S    Jul24   0:03 [migration/1]
root          22  0.0  0.0      0     0 ?        S    Jul24   0:24 [ksoftirqd/1]
root          24  0.0  0.0      0     0 ?        I<   Jul24   0:00 [kworker/1:0H-events_highpri]
root          25  0.0  0.0      0     0 ?        S    Jul24   0:00 [cpuhp/2]
root          26  0.0  0.0      0     0 ?        S    Jul24   0:00 [idle_inject/2]
root          27  0.0  0.0      0     0 ?        S    Jul24   0:01 [migration/2]
root          28  0.0  0.0      0     0 ?        S    Jul24   0:00 [ksoft [...]
```

## 152743 - Unix Software Discovery Commands Not Available

### Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

### Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.

Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

* Inadequate scan user permissions,

* Failed privilege escalation,

* Intermittent network disruption, or

* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

### Plugin Output

tcp/0

```
Failures in commands used to assess Unix software:

  unzip -v                    :
    sh: 1: unzip: not found


Account  : anapaya
Protocol : SSH
```

## 11154 - Unknown Service Detection: Banner Retrieval

### Synopsis

There is an unknown service running on the remote host.

### Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

### Plugin Output

tcp/30252

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port    : 30252
  Type    : spontaneous
  Banner :
0x00:  00 00 0C 04 00 00 00 00 00 00 05 00 00 40 00 00    .............@..
          0x10:  03 00 00 00 80                                        .....


Nessus detected the following process listening on this port :

/app/scion-all
```

## 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: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:

  Path    : /usr/bin/vim.tiny
  Version : 8.2

  Path    : /usr/bin/vim.basic
  Version : 8.2
```

## 91815 - Web Application Sitemap

### Synopsis

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

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/443/www

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

  - https://192.168.111.1/ui
  - https://192.168.111.1/ui/
  - https://192.168.111.1/ui/favicon.ico
  - https://192.168.111.1/ui/styles.f099f610cfe9907e.css

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

## 91815 - Web Application Sitemap

### Synopsis

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

### Description

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

### See Also

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

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

  - http://192.168.111.1:42001/

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

## 10386 - Web Server No 404 Error Code Check

### Synopsis

The remote web server does not return 404 error codes.

### Description

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

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

### Solution

n/a

### Risk Factor

None

### Plugin Information

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

### Plugin Output

tcp/42001/www

```
Unfortunately, Nessus has been unable to find a way to recognize this
page so some CGI-related checks have been disabled.
```

## 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.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: 2023/10/10, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 2 installs of libcurl:

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.7.0
  Version            : 7.81.0
  Associated Package : libcurl4 7.81.0-1ubuntu1.16
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.7.0
  Version            : 7.81.0
  Associated Package : libcurl3-gnutls 7.81.0-1ubuntu1.16
  Managed by OS      : True
```

# 192.168.112.1

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 1 | 10 | 10 | 9 | 108 |

## Scan Information

Start time: Mon Aug 12 13:48:32 2024

End time: Mon Aug 12 14:14:58 2024

## Host Information

IP: 192.168.112.1

MAC Address: 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95

OS: Linux Kernel 5.15.0-116-generic on Ubuntu 22.04

## Vulnerabilities

### 204924 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenSSL vulnerabilities (USN-6937-1)

#### Synopsis

The remote Ubuntu host is missing one or more security updates.

#### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6937-1 advisory.

It was discovered that OpenSSL incorrectly handled TLSv1.3 sessions when certain non-default TLS server configurations were in use. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. (CVE-2024-2511)

It was discovered that OpenSSL incorrectly handled checking excessively long DSA keys or parameters. A remote attacker could possibly use this issue to cause OpenSSL to consume resources, leading to a denial of service. This issue only affected Ubuntu 22.04 LTS and Ubuntu 24.04 LTS. (CVE-2024-4603)

William Ahern discovered that OpenSSL incorrectly handled certain memory operations in a rarely-used API.

A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service, or possibly execute arbitrary code. (CVE-2024-4741)

Joseph Birr-Pixton discovered that OpenSSL incorrectly handled calling a certain API with an empty supported client protocols buffer. A remote attacker could possibly use this issue to obtain sensitive information, or cause OpenSSL to crash, resulting in a denial of service. (CVE-2024-5535)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6937-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

6.0

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-2511 |
| CVE | CVE-2024-4603 |
| CVE | CVE-2024-4741 |
| CVE | CVE-2024-5535 |
| XREF | IAVA:2024-A-0208-S |
| XREF | IAVA:2024-A-0321 |
| XREF | USN:6937-1 |

## Plugin Information

Published: 2024/07/31, Modified: 2024/07/31

## Plugin Output

tcp/0

```
  - Installed package : libssl3_3.0.2-0ubuntu1.16
  - Fixed package     : libssl3_3.0.2-0ubuntu1.17

  - Installed package : openssl_3.0.2-0ubuntu1.16
  - Fixed package     : openssl_3.0.2-0ubuntu1.17
```

## 192704 - Curl 7.44.0 < 8.7.0 HTTP/2 Push Headers Memory-leak (CVE-2024-2398)

### Synopsis

The remote host has a program that is affected by a memory-leak vulnerability.

### Description

The version of Curl installed on the remote host is between 7.44.0 and prior to 8.7.0. It is, therefore, affected by a memory-leak vulnerability. When an application tells libcurl it wants to allow HTTP/2 server push, and the amount of received headers for the push surpasses the maximum allowed limit (1000), libcurl aborts the server push. When aborting, libcurl inadvertently does not free all the previously allocated headers and instead leaks the memory.

Further, this error condition fails silently and is therefore not easily detected by an application.

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

### See Also

https://curl.se/docs/CVE-2024-2398.html

### Solution

Upgrade Curl to version 8.7.0 or later

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.5

### EPSS Score

0.0005

### CVSS v2.0 Base Score

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

## CVSS v2.0 Temporal Score

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

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-2398 |
| XREF | IAVA:2024-A-0185-S |

## Plugin Information

Published: 2024/03/29, Modified: 2024/07/26

## Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/curl
  Installed version : 7.64.0
  Fixed version     : 8.7.0
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/bin/curl
  Installed version : 7.64.0
  Fixed version     : 8.7.0
```

## 205195 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos vulnerabilities (USN-6947-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6947-1 advisory.

It was discovered that Kerberos incorrectly handled GSS message tokens where an unwrapped token could appear to be truncated. An attacker could possibly use this issue to cause a denial of service.

(CVE-2024-37370)

It was discovered that Kerberos incorrectly handled GSS message tokens when sent a token with invalid length fields. An attacker could possibly use this issue to cause a denial of service. (CVE-2024-37371)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6947-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

5.2

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### References

| | |
|---|---|
| CVE | CVE-2024-37370 |
| CVE | CVE-2024-37371 |
| XREF | USN:6947-1 |

### Plugin Information

Published: 2024/08/08, Modified: 2024/08/08

### Plugin Output

tcp/0

```
- Installed package : libgssapi-krb5-2_1.19.2-2ubuntu0.3
- Fixed package     : libgssapi-krb5-2_1.19.2-2ubuntu0.4

- Installed package : libk5crypto3_1.19.2-2ubuntu0.3
- Fixed package     : libk5crypto3_1.19.2-2ubuntu0.4

- Installed package : libkrb5-3_1.19.2-2ubuntu0.3
- Fixed package     : libkrb5-3_1.19.2-2ubuntu0.4

- Installed package : libkrb5support0_1.19.2-2ubuntu0.3
- Fixed package     : libkrb5support0_1.19.2-2ubuntu0.4
```

## 185739 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : pip vulnerabilities (USN-6473-2)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6473-2 advisory.

- urllib3 before 1.24.2 does not remove the authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the authorization header to be exposed to unintended hosts or transmitted in cleartext. NOTE: this issue exists because of an incomplete fix for CVE-2018-20060 (which was case-sensitive). (CVE-2018-25091)

- urllib3 is a user-friendly HTTP client library for Python. urllib3 doesn't treat the `Cookie` HTTP header special or provide any helpers for managing cookies over HTTP, that is the responsibility of the user.

However, it is possible for a user to specify a `Cookie` header and unknowingly leak information via HTTP redirects to a different origin if that user doesn't disable redirects explicitly. This issue has been patched in urllib3 version 1.26.17 or 2.0.5. (CVE-2023-43804)

- urllib3 is a user-friendly HTTP client library for Python. urllib3 previously wouldn't remove the HTTP request body when an HTTP redirect response using status 301, 302, or 303 after the request had its method changed from one that could accept a request body (like `POST`) to `GET` as is required by HTTP RFCs.

Although this behavior is not specified in the section for redirects, it can be inferred by piecing together information from different sections and we have observed the behavior in other major HTTP client implementations like curl and web browsers. Because the vulnerability requires a previously trusted service to become compromised in order to have an impact on confidentiality we believe the exploitability of this vulnerability is low. Additionally, many users aren't putting sensitive data in HTTP request bodies, if this is the case then this vulnerability isn't exploitable. Both of the following conditions must be true to be affected by this vulnerability: 1. Using urllib3 and submitting sensitive information in the HTTP request body (such as form data or JSON) and 2. The origin service is compromised and starts redirecting using 301, 302, or 303 to a malicious peer or the redirected-to service becomes compromised.

This issue has been addressed in versions 1.26.18 and 2.0.7 and users are advised to update to resolve this issue. Users unable to update should disable redirects for services that aren't expecting to respond with redirects with `redirects=False` and disable automatic redirects with `redirects=False` and handle 301, 302, and 303 redirects manually by stripping the HTTP request body. (CVE-2023-45803)

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://ubuntu.com/security/notices/USN-6473-2

### Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.0

EPSS Score

0.0008

CVSS v2.0 Base Score

8.5 (CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:N)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2018-25091 |
| CVE | CVE-2023-43804 |
| CVE | CVE-2023-45803 |
| XREF | USN:6473-2 |

Plugin Information

Published: 2023/11/15, Modified: 2023/11/15

Plugin Output

tcp/0

```
- Installed package : python3-pip_22.0.2+dfsg-1ubuntu0.3
- Fixed package     : python3-pip_22.0.2+dfsg-1ubuntu0.4
```

## 195216 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6768-1 advisory.

- An issue was discovered in GNOME GLib before 2.78.5, and 2.79.x and 2.80.x before 2.80.1. When a GDBus- based client subscribes to signals from a trusted system service such as NetworkManager on a shared computer, other users of the same computer can send spoofed D-Bus signals that the GDBus-based client will wrongly interpret as having been sent by the trusted system service. This could lead to the GDBus-based client behaving incorrectly, with an application-dependent impact. (CVE-2024-34397)

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

### See Also

https://ubuntu.com/security/notices/USN-6768-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

2.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2024-34397 |
| XREF | USN:6768-1 |

Plugin Information

Published: 2024/05/09, Modified: 2024/05/09

Plugin Output

tcp/0

```
  - Installed package : libglib2.0-data_2.72.4-0ubuntu2.2
  - Fixed package     : libglib2.0-data_2.72.4-0ubuntu2.3
```

## 204989 - Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-6944-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6944-1 advisory.

Dov Murik discovered that curl incorrectly handled parsing ASN.1 Generalized Time fields. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly obtain sensitive memory contents.

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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

### See Also

https://ubuntu.com/security/notices/USN-6944-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

### VPR Score

3.9

### EPSS Score

0.0004

### CVSS v2.0 Base Score

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

### CVSS v2.0 Temporal Score

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

### STIG Severity

I

### References

| | |
|---|---|
| CVE | CVE-2024-7264 |
| XREF | IAVA:2024-A-0457 |
| XREF | USN:6944-1 |

### Plugin Information

Published: 2024/08/05, Modified: 2024/08/05

### Plugin Output

tcp/0

```
- Installed package : curl_7.81.0-1ubuntu1.16
- Fixed package     : curl_7.81.0-1ubuntu1.17

- Installed package : libcurl3-gnutls_7.81.0-1ubuntu1.16
- Fixed package     : libcurl3-gnutls_7.81.0-1ubuntu1.17

- Installed package : libcurl4_7.81.0-1ubuntu1.16
- Fixed package     : libcurl4_7.81.0-1ubuntu1.17
```

## 204913 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6923-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6923-1 advisory.

Benedict Schlter, Supraja Sridhara, Andrin Bertschi, and Shweta Shinde discovered that an untrusted hypervisor could inject malicious #VC interrupts and compromise the security guarantees of AMD SEV-SNP.

This flaw is known as WeSee. A local attacker in control of the hypervisor could use this to expose sensitive information or possibly execute arbitrary code in the trusted execution environment.

(CVE-2024-25742)

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- TTY drivers;

- SMB network file system;

- Netfilter;

- Bluetooth subsystem; (CVE-2024-26886, CVE-2024-26952, CVE-2023-52752, CVE-2024-27017, CVE-2024-36016)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6923-1

### Solution

Update the affected kernel package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0004

CVSS v2.0 Base Score

6.8 (CVSS2#AV:L/AC:L/Au:S/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

| | |
|---|---|
| CVE | CVE-2023-52752 |
| CVE | CVE-2024-25742 |
| CVE | CVE-2024-26886 |
| CVE | CVE-2024-26952 |
| CVE | CVE-2024-27017 |
| CVE | CVE-2024-36016 |
| XREF | USN:6923-1 |

Plugin Information

Published: 2024/07/31, Modified: 2024/07/31

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-116-generic does not meet the minimum fixed level of 5.15.0-117-
generic for this advisory.
```

## 189773 - Ubuntu 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-6616-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6616-1 advisory.

- A vulnerability was found in openldap. This security flaw causes a null pointer dereference in ber_memalloc_x() function. (CVE-2023-2953)

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

### See Also

https://ubuntu.com/security/notices/USN-6616-1

### Solution

Update the affected packages.

### Risk Factor

High

### CVSS v3.0 Base Score

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

### CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

4.4

### EPSS Score

0.0039

### CVSS v2.0 Base Score

7.8 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

5.8 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2023-2953 |
| XREF | USN:6616-1 |

## Plugin Information

Published: 2024/01/30, Modified: 2024/01/30

## Plugin Output

tcp/0

```
  - Installed package : libldap-common_2.5.16+dfsg-0ubuntu0.22.04.1
  - Fixed package     : libldap-common_2.5.16+dfsg-0ubuntu0.22.04.2
```

## 204858 - Ubuntu 20.04 LTS / 22.04 LTS : Python vulnerabilities (USN-6928-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6928-1 advisory.

It was discovered that the Python ssl module contained a memory race condition when handling the APIs to obtain the CA certificates and certificate store statistics. This could possibly result in applications obtaining wrong results, leading to various SSL issues. (CVE-2024-0397)

It was discovered that the Python ipaddress module contained incorrect information about which IP address ranges were considered private or globally reachable. This could possibly result in applications applying incorrect security policies. (CVE-2024-4032)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6928-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H)

### CVSS v3.0 Temporal Score

6.4 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

6.0

### EPSS Score

0.0005

## CVSS v2.0 Base Score

4.0 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:P)

## CVSS v2.0 Temporal Score

3.0 (CVSS2#E:U/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2024-0397 |
| CVE | CVE-2024-4032 |
| XREF | USN:6928-1 |

## Plugin Information

Published: 2024/07/30, Modified: 2024/07/30

## Plugin Output

tcp/0

```
- Installed package : libpython3.10_3.10.12-1~22.04.4
- Fixed package     : libpython3.10_3.10.12-1~22.04.5

- Installed package : libpython3.10-minimal_3.10.12-1~22.04.4
- Fixed package     : libpython3.10-minimal_3.10.12-1~22.04.5

- Installed package : libpython3.10-stdlib_3.10.12-1~22.04.4
- Fixed package     : libpython3.10-stdlib_3.10.12-1~22.04.5

- Installed package : python3.10_3.10.12-1~22.04.4
- Fixed package     : python3.10_3.10.12-1~22.04.5

- Installed package : python3.10-minimal_3.10.12-1~22.04.4
- Fixed package     : python3.10-minimal_3.10.12-1~22.04.5
```

## 150154 - nginx 0.6.x < 1.20.1 1-Byte Memory Overwrite RCE

### Synopsis

The remote web server is affected by a remote code execution vulnerability.

### Description

According to its Server response header, the installed version of nginx is 0.6.18 prior to 1.20.1. It is, therefore, affected by a remote code execution vulnerability. A security issue in nginx resolver was identified, which might allow an unauthenticated remote attacker to cause 1-byte memory overwrite by using a specially crafted DNS response, resulting in worker process crash or, potentially, in arbitrary code execution.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html

http://nginx.org/download/patch.2021.resolver.txt

### Solution

Upgrade to nginx 1.20.1 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

7.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L)

### CVSS v3.0 Temporal Score

6.9 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

7.0

### EPSS Score

0.3895

### CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## CVSS v2.0 Temporal Score

5.3 (CVSS2#E:POC/RL:OF/RC:C)

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2021-23017 |
| XREF | IAVB:2021-B-0031 |
| XREF | CWE:193 |

## Plugin Information

Published: 2021/06/03, Modified: 2022/09/15

## Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/sbin/nginx
  Installed version : 1.19.9
  Fixed version     : 1.20.1 / 1.21.0
```

## 187725 - Curl 7.46.0 <= 8.4.0 Information Disclosure (CVE-2023-46218)

### Synopsis

The remote host has a program that is affected by an information disclosure vulnerability.

### Description

The version of Curl installed on the remote host is between 7.46.0 and 8.4.0. It is, therefore, affected by an information disclosure vulnerability. A mixed case flaw in Curl's function that verifies a given cookie domain against the Public Suffix List (PSL) allows a malicious HTTP server to set 'super cookies' in Curl, that are then passed back to more origins than what is otherwise allowed or possible. For example a cookie could be set with `domain=co.UK` when the URL used a lower case hostname `curl.co.uk`, even though `co.uk` is listed as a PSL domain.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://curl.se/docs/CVE-2023-46218.html

### Solution

Upgrade Curl to version 8.5.0 or later

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v3.0 Temporal Score

5.9 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

3.3

### EPSS Score

0.0007

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## CVSS v2.0 Temporal Score

5.0 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2023-46218 |

## Plugin Information

Published: 2024/01/09, Modified: 2024/04/19

## Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/curl
  Installed version : 7.64.0
  Fixed version     : 8.5.0
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/bin/curl
  Installed version : 7.64.0
  Fixed version     : 8.5.0
```

## 51192 - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

### Solution

Purchase or generate a proper SSL certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

## Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

## Plugin Output

tcp/443/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=Caddy Local Authority - ECC Intermediate
|-Issuer  : CN=Caddy Local Authority - 2023 ECC Root
```

## 190598 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability (USN-6640-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6640-1 advisory.

- A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.

(CVE-2023-4641)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://ubuntu.com/security/notices/USN-6640-1

### Solution

Update the affected packages.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:C/I:N/A:N)

### CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| CVE | CVE-2023-4641 |
| XREF | USN:6640-1 |

### Plugin Information

Published: 2024/02/15, Modified: 2024/02/15

### Plugin Output

tcp/0

```
  - Installed package : login_1:4.8.1-2ubuntu2.1
  - Fixed package     : login_1:4.8.1-2ubuntu2.2
```

## 185568 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM host has a package installed that is affected by a vulnerability as referenced in the USN-6478-1 advisory.

- In buc Traceroute 2.0.12 through 2.1.2 before 2.1.3, the wrapper scripts do not properly parse command lines. (CVE-2023-46316)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://ubuntu.com/security/notices/USN-6478-1

### Solution

Update the affected traceroute package.

### Risk Factor

Medium

### CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

### CVSS v3.0 Temporal Score

5.0 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

## CVSS v2.0 Temporal Score

3.6 (CVSS2#E:POC/RL:OF/RC:C)

## References

| | |
|---|---|
| CVE | CVE-2023-46316 |
| XREF | USN:6478-1 |

## Plugin Information

Published: 2023/11/14, Modified: 2024/01/23

## Plugin Output

tcp/0

```
  - Installed package : traceroute_1:2.1.0-2
  - Fixed package     : traceroute_1:2.1.0-2ubuntu0.22.04.1~esm1


NOTE: The fixed ESM package referenced in this plugin requires a
subscription to Ubuntu Pro to enable the ESM repositories.
```

## 205227 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6950-1)

### Synopsis

The remote Ubuntu host is missing one or more security updates.

### Description

The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6950-1 advisory.

Several security issues were discovered in the Linux kernel. An attacker could possibly use these to compromise the system. This update corrects flaws in the following subsystems:

- ARM32 architecture;

- ARM64 architecture;

- Block layer subsystem;

- Bluetooth drivers;

- Clock framework and drivers;

- FireWire subsystem;

- GPU drivers;

- InfiniBand drivers;

- Multiple devices driver;

- EEPROM drivers;

- Network drivers;

- Pin controllers subsystem;

- Remote Processor subsystem;

- S/390 drivers;

- SCSI drivers;

- 9P distributed file system;

- Network file system client;

- SMB network file system;

- Socket messages infrastructure;

- Dynamic debug library;

- Bluetooth subsystem;

- Networking core;

- IPv4 networking;

- IPv6 networking;

- Multipath TCP;

- NSH protocol;

- Phonet protocol;

- TIPC protocol;

- Wireless networking;

- Key management;

- ALSA framework;

- HD-audio driver; (CVE-2024-36883, CVE-2024-36940, CVE-2024-36902, CVE-2024-36975, CVE-2024-36964, CVE-2024-36938, CVE-2024-36931, CVE-2024-35848, CVE-2024-26900, CVE-2024-36967, CVE-2024-36904, CVE-2024-27398, CVE-2024-36031, CVE-2023-52585, CVE-2024-36886, CVE-2024-36937, CVE-2024-36954, CVE-2024-36916, CVE-2024-36905, CVE-2024-36959, CVE-2024-26980, CVE-2024-26936, CVE-2024-36928, CVE-2024-36889, CVE-2024-36929, CVE-2024-36933, CVE-2024-27399, CVE-2024-36946, CVE-2024-36906, CVE-2024-36965, CVE-2024-36957, CVE-2024-36941, CVE-2024-36897, CVE-2024-36952, CVE-2024-36947, CVE-2024-36950, CVE-2024-36880, CVE-2024-36017, CVE-2023-52882, CVE-2024-36969, CVE-2024-38600, CVE-2024-36955, CVE-2024-36960, CVE-2024-27401, CVE-2024-36919, CVE-2024-36934, CVE-2024-35947, CVE-2024-36953, CVE-2024-36944, CVE-2024-36939)

Tenable has extracted the preceding description block directly from the Ubuntu security advisory.

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://ubuntu.com/security/notices/USN-6950-1

## Solution

Update the affected kernel package.

## Risk Factor

Medium

## CVSS v3.0 Base Score

5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

## CVSS v3.0 Temporal Score

4.8 (CVSS:3.0/E:U/RL:O/RC:C)

## VPR Score

7.4

EPSS Score

0.0005

CVSS v2.0 Base Score

4.6 (CVSS2#AV:L/AC:L/Au:S/C:N/I:N/A:C)

CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

References

| | |
|---|---|
| CVE | CVE-2023-52585 |
| CVE | CVE-2023-52882 |
| CVE | CVE-2024-26900 |
| CVE | CVE-2024-26936 |
| CVE | CVE-2024-26980 |
| CVE | CVE-2024-27398 |
| CVE | CVE-2024-27399 |
| CVE | CVE-2024-27401 |
| CVE | CVE-2024-35848 |
| CVE | CVE-2024-35947 |
| CVE | CVE-2024-36017 |
| CVE | CVE-2024-36031 |
| CVE | CVE-2024-36880 |
| CVE | CVE-2024-36883 |
| CVE | CVE-2024-36886 |
| CVE | CVE-2024-36889 |
| CVE | CVE-2024-36897 |
| CVE | CVE-2024-36902 |
| CVE | CVE-2024-36904 |
| CVE | CVE-2024-36905 |
| CVE | CVE-2024-36906 |
| CVE | CVE-2024-36916 |
| CVE | CVE-2024-36919 |
| CVE | CVE-2024-36928 |
| CVE | CVE-2024-36929 |
| CVE | CVE-2024-36931 |
| CVE | CVE-2024-36933 |
| CVE | CVE-2024-36934 |
| CVE | CVE-2024-36937 |

| | |
|---|---|
| CVE | CVE-2024-36938 |
| CVE | CVE-2024-36939 |
| CVE | CVE-2024-36940 |
| CVE | CVE-2024-36941 |
| CVE | CVE-2024-36944 |
| CVE | CVE-2024-36946 |
| CVE | CVE-2024-36947 |
| CVE | CVE-2024-36950 |
| CVE | CVE-2024-36952 |
| CVE | CVE-2024-36953 |
| CVE | CVE-2024-36954 |
| CVE | CVE-2024-36955 |
| CVE | CVE-2024-36957 |
| CVE | CVE-2024-36959 |
| CVE | CVE-2024-36960 |
| CVE | CVE-2024-36964 |
| CVE | CVE-2024-36965 |
| CVE | CVE-2024-36967 |
| CVE | CVE-2024-36969 |
| CVE | CVE-2024-36975 |
| CVE | CVE-2024-38600 |
| XREF | USN:6950-1 |

## Plugin Information

Published: 2024/08/08, Modified: 2024/08/08

## Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-116-generic does not meet the minimum fixed level of 5.15.0-118-
generic for this advisory.
```

## 200807 - urllib3 Python Library < 1.26.19, < 2.2.2 (CVE-2024-37891)

### Synopsis

A Python library installed on the remote host is affected by a vulnerability.

### Description

urllib3 is a user-friendly HTTP client library for Python. When using urllib3's proxy support with 'ProxyManager', the 'Proxy-Authorization' header is only sent to the configured proxy, as expected. However, when sending HTTP requests without using urllib3's proxy support, it's possible to accidentally configure the 'Proxy-Authorization' header even though it won't have any effect as the request is not using a forwarding proxy or a tunneling proxy. In those cases, urllib3 doesn't treat the 'Proxy-Authorization' HTTP header as one carrying authentication material and thus doesn't strip the header on cross-origin redirects.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

http://www.nessus.org/u?7b44847c

### Solution

Upgrade to urllib3 version 1.26.19, 2.2.2 or later.

### Risk Factor

Medium

### CVSS v3.0 Base Score

4.4 (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N)

### CVSS v3.0 Temporal Score

3.9 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

4.4

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.6 (CVSS2#AV:N/AC:H/Au:M/C:C/I:N/A:N)

## CVSS v2.0 Temporal Score

3.4 (CVSS2#E:U/RL:OF/RC:C)

## STIG Severity

II

## References

| | |
|---|---|
| CVE | CVE-2024-37891 |
| XREF | IAVA:2024-A-0363 |

## Plugin Information

Published: 2024/06/21, Modified: 2024/07/15

## Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/usr/lib/python3.8/
site-packages/urllib3
  Installed version : 1.26.2
  Fixed version     : 1.26.19
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9b912a9a533b1bc2ab6cff1fc4247ca836d16954283b017a7c7da55a83fad17/diff/usr/local/lib/python3.8/site-
packages/urllib3
  Installed version : 1.26.3
  Fixed version     : 1.26.19
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/l/KYYSYAFSY3IVQOAFWPEZDFRHYS/usr/lib/python3.8/site-
packages/urllib3
  Installed version : 1.26.2
  Fixed version     : 1.26.19
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/l/L6YZICRJK53S6YZVXMBLBVCZKI/usr/local/lib/python3.8/
site-packages/urllib3
  Installed version : 1.26.3
  Fixed version     : 1.26.19
```

## 205023 - Curl 7.32.0 < 8.9.1 DoS (CVE-2024-7264)

### Synopsis

The remote host has a program that is affected by a DoS vulnerability.

### Description

The version of Curl installed on the remote host is between 7.32.0 and prior to 8.9.1. It is, therefore, affected by a denial of service (DoS) vulnerability. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the time fraction, leading to a strlen() getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://curl.se/docs/CVE-2024-7264.html

### Solution

Upgrade Curl to version 8.9.1 or later

### Risk Factor

Medium

### CVSS v3.0 Base Score

3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L)

### CVSS v3.0 Temporal Score

2.7 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

3.9

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

## CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-7264 |
| XREF | IAVA:2024-A-0457 |

## Plugin Information

Published: 2024/08/06, Modified: 2024/08/07

## Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/curl
  Installed version : 7.64.0
  Fixed version     : 8.9.1
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/bin/curl
  Installed version : 7.64.0
  Fixed version     : 8.9.1
```

## 10114 - ICMP Timestamp Request Remote Date Disclosure

### Synopsis

It is possible to determine the exact time set on the remote host.

### Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.

Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

### Solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

### Risk Factor

Low

### VPR Score

4.2

### EPSS Score

0.8808

### CVSS v2.0 Base Score

2.1 (CVSS2#AV:L/AC:L/Au:N/C:P/I:N/A:N)

### References

| | |
|---|---|
| CVE | CVE-1999-0524 |
| XREF | CWE:200 |

### Plugin Information

Published: 1999/08/01, Modified: 2024/05/03

### Plugin Output

icmp/0

```
The remote clock is synchronized with the local clock.
```

## 205024 - libcurl 7.32.0 < 8.9.1 DoS (CVE-2024-7264)

### Synopsis

The remote host contains a version of libcurl that is affected by a DoS vulnerability.

### Description

The version of libcurl installed on the remote host is between 7.32.0 and prior to 8.9.1. It is, therefore, affected by a denial of service (DoS) vulnerability. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the time fraction, leading to a strlen() getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://curl.se/docs/CVE-2024-7264.html

### Solution

Upgrade Curl to version 8.9.1 or later

### Risk Factor

Medium

### CVSS v3.0 Base Score

3.1 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L)

### CVSS v3.0 Temporal Score

2.7 (CVSS:3.0/E:U/RL:O/RC:C)

### VPR Score

3.9

### EPSS Score

0.0004

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

## CVSS v2.0 Temporal Score

3.2 (CVSS2#E:U/RL:OF/RC:C)

## STIG Severity

I

## References

| | |
|---|---|
| CVE | CVE-2024-7264 |
| XREF | IAVA:2024-A-0457 |

## Plugin Information

Published: 2024/08/06, Modified: 2024/08/07

## Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/121ad0592b404cd784e8de1bb8896462fdbee25e117e116dcb8e1deaee5ffa68/diff/usr/lib/x86_64-linux-
gnu/libcurl-gnutls.so.4.5.0
  Installed version : 7.64.0
  Fixed version     : 8.9.1
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0
  Installed version : 7.64.0
  Fixed version     : 8.9.1
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libcurl.so.4.5.0
  Installed version : 7.64.0
  Fixed version     : 8.9.1
```

## 182873 - libcurl 7.9.1 < 8.4.0 Cookie Injection

### Synopsis

The remote libcurl install is affected by a cookie injection vulnerability.

### Description

The version of libcurl installed on the remote host is affected by a cookie injection vulnerability. This flaw allows an attacker to insert cookies at will into a running program using libcurl, if the specific series of conditions are met.

libcurl performs transfers. In its API, an application creates 'easy handles' that are the individual handles for single transfers.

libcurl provides a function call that duplicates an easy handle called curl_easy_duphandle.

If a transfer has cookies enabled when the handle is duplicated, the cookie-enable state is also cloned - but without cloning the actual cookies. If the source handle did not read any cookies from a specific file on disk, the cloned version of the handle would instead store the file name as none (using the four ASCII letters, no quotes).

Subsequent use of the cloned handle that does not explicitly set a source to load cookies from would then inadvertently load cookies from a file named none - if such a file exists and is readable in the current directory of the program using libcurl. And if using the correct file format of course.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://curl.se/docs/CVE-2023-38546.html

### Solution

Upgrade libcurl to version 8.4.0 or later

### Risk Factor

Low

### CVSS v3.0 Base Score

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

### CVSS v3.0 Temporal Score

3.4 (CVSS:3.0/E:P/RL:O/RC:C)

### VPR Score

2.9

EPSS Score

0.0008

CVSS v2.0 Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N)

CVSS v2.0 Temporal Score

2.0 (CVSS2#E:POC/RL:OF/RC:C)

STIG Severity

I

References

| | |
|---|---|
| CVE | CVE-2023-38546 |
| XREF | CEA-ID:CEA-2023-0052 |
| XREF | IAVA:2023-A-0531-S |

Plugin Information

Published: 2023/10/11, Modified: 2023/12/08

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/121ad0592b404cd784e8de1bb8896462fdbee25e117e116dcb8e1deaee5ffa68/diff/usr/lib/x86_64-linux-
gnu/libcurl-gnutls.so.4.5.0
  Installed version : 7.64.0
  Fixed version     : 8.4.0
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0
  Installed version : 7.64.0
  Fixed version     : 8.4.0
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libcurl.so.4.5.0
  Installed version : 7.64.0
  Fixed version     : 8.4.0
```

## 156000 - Apache Log4j Installed (Linux / Unix)

### Synopsis

Apache Log4j, a logging API, is installed on the remote Linux / Unix host.

### Description

One or more instances of Apache Log4j, a logging API, are installed on the remote Linux / Unix Host.

The plugin timeout can be set to a custom value other than the plugin's default of 45 minutes via the 'timeout.156000' scanner setting in Nessus 8.15.1 or later.

Please see https://docs.tenable.com/nessus/Content/SettingsAdvanced.htm#Custom for more information.

### See Also

https://logging.apache.org/log4j/2.x/

### Solution

n/a

### Risk Factor

None

### References

| | |
|---|---|
| XREF | IAVA:0001-A-0650 |
| XREF | IAVT:0001-T-0941 |

### Plugin Information

Published: 2021/12/10, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 2 installs of Apache Log4j:

  Path                           : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/share/java/
libintl.jar
  Version                        : unknown
  JMSAppender.class association  : Not Found
  JdbcAppender.class association : Not Found
  JndiLookup.class association   : Not Found
  Method                         : Embedded string inspection
```

```
  Path                           : /usr/share/java/libintl-0.21.jar
  Version                        : unknown
  JMSAppender.class association  : Not Found
  JdbcAppender.class association : Not Found
  JndiLookup.class association   : Not Found
  Method                         : Embedded string inspection


Note: Jar file inspection cannot be performed.  No results or cannot list archive contents.  If
 results are present, install an unzip package to resolve this problem.
```

## 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      : FNCB1515F00006W111
Vendor       : American Megatrends Inc.
Release Date : 09/28/2020
UUID         : 03000200-0400-0500-0006-000700080009
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: 2024/07/31

### Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:22.04 -> Canonical Ubuntu Linux

Following application CPE's matched on the remote system :

  cpe:/a:apache:log4j -> Apache Software Foundation log4j
  cpe:/a:docker:docker:27.1.1 -> Docker
  cpe:/a:gnupg:libgcrypt:1.8.4 -> GnuPG Libgcrypt
  cpe:/a:gnupg:libgcrypt:1.8.8 -> GnuPG Libgcrypt
  cpe:/a:gnupg:libgcrypt:1.9.4 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.64.0 -> Haxx Curl
  cpe:/a:haxx:curl:7.81.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.64.0 -> Haxx libcurl
  cpe:/a:haxx:libcurl:7.81.0 -> Haxx libcurl
  cpe:/a:nginx:nginx:1.19.9 -> Nginx
  cpe:/a:openbsd:openssh:8.9 -> OpenBSD OpenSSH
  cpe:/a:openbsd:openssh:8.9p1 -> OpenBSD OpenSSH
```

```
    cpe:/a:sqlite:sqlite -> SQLite
    cpe:/a:tukaani:xz -> Tukaani XZ
    cpe:/a:tukaani:xz:5.2.4 -> Tukaani XZ
    cpe:/a:tukaani:xz:5.2.5 -> Tukaani XZ
    cpe:/a:tukaani:xz:5.4.3 -> Tukaani XZ
    cpe:/a:vim:vim:8.2 -> 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: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 3 installs of Curl:

  Path    : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/bin/curl
  Version : 7.64.0

  Path    : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/curl
  Version : 7.64.0

  Path               : /usr/bin/curl
  Version            : 7.81.0
```

```
    Associated Package : curl 7.81.0-1ubuntu1.16
    Managed by OS      : True
```

## 132634 - Deprecated SSLv2 Connection Attempts

### Synopsis

Secure Connections, using a deprecated protocol were attempted as part of the scan

### Description

This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities and most major ssl libraries such as openssl, nss, mbed and wolfssl do not provide this functionality in their latest versions. This protocol has been deprecated in Nessus 8.9 and later.

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/01/06, Modified: 2020/01/06

### Plugin Output

tcp/0

```
Nessus attempted the following SSLv2 connection(s) as part of this scan:

Plugin ID: 42476
Timestamp: 2024-08-12 11:50:01
Port: 22
```

## 55472 - Device Hostname

### Synopsis

It was possible to determine the remote system hostname.

### Description

This plugin reports a device's hostname collected via SSH or WMI.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/06/30, Modified: 2024/08/06

### Plugin Output

tcp/0

```
Hostname : s01-chlau1-arma
  s01-chlau1-arma (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 : 100
```

## 111529 - Docker Container Number of Changed Files

### Synopsis

Checks for changes in running Docker containers and reports how many files changed.

### Description

This plugin checks the docker diff information for each container and reports the number of changed files.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/08/03, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Docker container b59f8e6724bebc52083e79123e658955eb11ba74ae54e40daf5ebcb541993f28 has 7 changed
 files

Docker container a12419dc636ea33779a983e35a833264bcddab11b897b73e5923b96c5a54e7ce has 26 changed
 files

Docker container abfc5306ce1e5fc9b58cc75ba4a735f28b483ce73e86a6c03bb5ee20f102bc72 has 18 changed
 files

Docker container 1c3df73950dbd6094906567b1629b4ec033b32884be7220d2ca2c43cdd296ca4 has 6 changed
 files

Docker container 9637fd621999ea15fe7c327b2dac36a95860143ddd264d85397e089fad4a7ca1 has 6 changed
 files

Docker container b7abfb368e7f1bb70be8bc93e4b243188c184107a94646ffe3595f206a0a4270 has 9 changed
 files

Docker container 8630f0d45e125660dc6858a25dc3397335ac63a8ccacefa8932aa45ebf710c60 has 6 changed
 files

Docker container 511400d85d4f93526197748909f3583fc35ae7abb0a9266ccb96b26a2adf6f13 has 3 changed
 files
```

```
Docker container 3b3272a921533f6c6e284206d5e6865389808c17b3464f1d66e49410ddf20abf has 5 changed
 files

Docker container 678d4069aaf4eab58d70d60a6fd7408976b59e3342b9b98331a2c67109a198e2 has 14 changed
 files

Docker container 774d0340089acf7fc44d9d043ef95a55544907a31c9c286efa0c8d4c73aa8f80 has 6 changed
 files
```

## 159488 - Docker Installed (Linux)

### Synopsis

Docker was detected on the remote host.

### Description

A container virtualization suite is installed on the remote host.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/04, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Path    : /usr/bin/docker
Version : 27.1.1
build   : 6312585
```

## 93561 - Docker Service Detection

### Synopsis

Docker was detected on the remote host.

### Description

The Docker service is running on the remote host. Docker is an open-source project that automates the deployment of applications inside software containers.

### See Also

https://www.docker.com/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/09/16, Modified: 2024/08/08

### Plugin Output

tcp/0

```
  Version: 27.1.1
  Version: 27.1.1
  Version: 1.7.19
  Version: 1.7.19
  Version: 0.19.0

The following containers were detected running on the remote Docker host :

Name:      /dataplane-control
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        b59f8e6724bebc52083e79123e658955eb11ba74ae54e40daf5ebcb541993f28
Ports:     n/a

Name:      /control-64-2_0_2d
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        a12419dc636ea33779a983e35a833264bcddab11b897b73e5923b96c5a54e7ce
Ports:     n/a

Name:      /dataplane
Image:     vpp-dataplane
```

```
Image ID : sha256:c30fa9fd28754cc2328e51f64f4b05aa56aee255f98d5b6c4b3952b75e22f50d
Tag:       v0.36.3
ID:        abfc5306ce1e5fc9b58cc75ba4a735f28b483ce73e86a6c03bb5ee20f102bc72
Ports:     n/a

Name:      /promtail
Image:     promtail
Image ID : sha256:c19fe7a93bf0b034b2f455962c53267dc56c02613f22788188a63f60c98638e8
Tag:       v0.36.3
ID:        1c3df73950dbd6094906567b1629b4ec033b32884be7220d2ca2c43cdd296ca4
Ports:     n/a

Name:      /gateway
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        9637fd621999ea15fe7c327b2dac36a95860143ddd264d85397e089fad4a7ca1
Ports:     n/a

Name:      /appliance-cron
Image:     appliance
Image ID : sha256:e10607406bb6806690db889fdf91e7332bf652d15529798846c46244de03d2eb
Tag:       v0.36.3
ID:        b7abfb368e7f1bb70be8bc93e4b243188c184107a94646ffe3595f206a0a4270
Ports:     n/a

Name:      /router
Image:     scion-all
Image ID : sha256:a970c5eb1eb475f4c117c5b98f81a08300765e906e66c9e87aa91ab3f79a26a4
Tag:       v0.36.3
ID:        8630f0d45e125660dc6858a25dc3397335ac63a8ccacefa8932aa45ebf710c60
Ports:     n/a

Name:      /telemetry
Image:     opentelemetry-collector
Image ID : sha256:1664fef5e8077e3c42f917dacd7aba8b339d6c9925cd5c9d6d7cee2e0d1d4ce7
Tag:       v0.36.3
ID:        511400d85d4f935261977489O9f3 [...]
```

## 159273 - Dockerfile Detection for Linux/UNIX

### Synopsis

Detected Dockerfiles on the host.

### Description

The host contains Dockerfiles, text files containing instructions to build Docker images.

### See Also

https://docs.docker.com/engine/reference/builder/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/03/29, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Dockerfiles found: 10
 - /var/lib/docker/overlay2/74787463fc4e131a9261a773db832865357bec0c9a42290aa195453f3619e5af/diff/
opt/certbot/tools/docker/plugin/Dockerfile
 - /var/lib/docker/overlay2/74787463fc4e131a9261a773db832865357bec0c9a42290aa195453f3619e5af/diff/
opt/certbot/tools/docker/core/Dockerfile
 - /var/lib/docker/overlay2/24b4dedd0616ab4bed5268e06009ae369390d7385053b268d0aea7c70e61a6f1/diff/
go/src/github.com/prometheus/alertmanager/vendor/golang.org/x/net/http2/Dockerfile
 - /var/lib/docker/overlay2/24b4dedd0616ab4bed5268e06009ae369390d7385053b268d0aea7c70e61a6f1/diff/
go/src/github.com/prometheus/alertmanager/Dockerfile
 - /var/lib/docker/overlay2/24b4dedd0616ab4bed5268e06009ae369390d7385053b268d0aea7c70e61a6f1/diff/
go/src/github.com/prometheus/alertmanager/ui/Dockerfile
 - /var/lib/docker/overlay2/l/UDE7KNIBXEZ3EVWJASW7KCKXYL/go/src/github.com/prometheus/alertmanager/
vendor/golang.org/x/net/http2/Dockerfile
 - /var/lib/docker/overlay2/l/UDE7KNIBXEZ3EVWJASW7KCKXYL/go/src/github.com/prometheus/alertmanager/
Dockerfile
 - /var/lib/docker/overlay2/l/UDE7KNIBXEZ3EVWJASW7KCKXYL/go/src/github.com/prometheus/alertmanager/
ui/Dockerfile
 - /var/lib/docker/overlay2/l/GFIIZPKFATHH2MHLZHAJYT53CF/opt/certbot/tools/docker/plugin/Dockerfile
 - /var/lib/docker/overlay2/l/GFIIZPKFATHH2MHLZHAJYT53CF/opt/certbot/tools/docker/core/Dockerfile
```

## 25203 - Enumerate IPv4 Interfaces via SSH

### Synopsis

Nessus was able to enumerate the IPv4 interfaces on the remote host.

### Description

Nessus was able to enumerate the network interfaces configured with IPv4 addresses by connecting to the remote host via SSH using the supplied credentials.

### Solution

Disable any unused IPv4 interfaces.

### Risk Factor

None

### Plugin Information

Published: 2007/05/11, Modified: 2024/02/05

### Plugin Output

tcp/0

```
The following IPv4 addresses are set on the remote host :

 - 172.17.0.1 (on interface docker0)
 - 192.168.112.1 (on interface enp10s0f1)
 - 10.110.192.49 (on interface enp2s0f0)
 - 127.0.0.1 (on interface lo)
 - 198.18.30.3 (on interface wg0)
```

## 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 :

 - fe80::290:bff:fea5:d295 (on interface enp10s0f1)
 - fe80::290:bff:fea5:d28e (on interface enp2s0f0)
 - ::1 (on interface lo)
 - fe80::ca8e:c258:f7cb:b9e8 (on interface scion-gateway)
```

## 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 :

  - 00:90:0b:a5:d2:91 (interface enp2s0f3)
  - 00:90:0b:a5:d2:8f (interface enp2s0f1)
  - 00:90:0b:a5:d2:93 (interface enp8s0f1)
  - 00:90:0b:a5:d2:8e (interface enp2s0f0)
  - 00:90:0b:a5:d2:90 (interface enp2s0f2)
  - 00:90:0b:a5:d2:92 (interface enp8s0f0)
  - 02:42:c7:7b:2b:aa (interface docker0)
  - 00:90:0b:a5:d2:94 (interface enp10s0f0)
  - 00:90:0b:a5:d2:95 (interface enp10s0f1)
```

## 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

```
enp2s0f3:
  MAC : 00:90:0b:a5:d2:91
enp8s0f0:
  MAC : 00:90:0b:a5:d2:92
enp2s0f1:
  MAC : 00:90:0b:a5:d2:8f
enp10s0f0:
  MAC : 00:90:0b:a5:d2:94
enp10s0f1:
  MAC : 00:90:0b:a5:d2:95
  IPv4:
    - Address : 192.168.112.1
      Netmask : 255.255.255.0
      Broadcast : 192.168.112.255
  IPv6:
    - Address : fe80::290:bff:fea5:d295
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
enp8s0f1:
  MAC : 00:90:0b:a5:d2:93
enp2s0f0:
  MAC : 00:90:0b:a5:d2:8e
  IPv4:
    - Address : 10.110.192.49
      Netmask : 255.255.255.252
      Broadcast : 10.110.192.51
  IPv6:
    - Address : fe80::290:bff:fea5:d28e
      Prefixlen : 64
      Scope : link
      ScopeID : 0x20
```

```
wg0:
  IPv4:
    - Address : 198.18.30.3
        Netmask : 255.255.255.255
scion-gateway:
  IPv6:
    - Address : fe80::ca8e:c258:f7cb:b9e8
        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
docker0:
  MAC : 02:42:c7:7b:2b:aa
  IPv4:
    - Address : 172.17.0.1
        Netmask : 255.255.0.0
        Broadcast : 172.17.255.255
enp2s0f2:
  MAC : 00:90:0b:a5:d2:90
```

## 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:
  wg0:
    ipv4_gateways:
      198.18.0.1:
        subnets:
          - 198.18.0.0/24
Interface Routes:
  docker0:
    ipv4_subnets:
      - 172.17.0.0/16
  enp10s0f1:
    ipv4_subnets:
      - 192.168.112.0/24
    ipv6_subnets:
      - fe80::/64
  enp2s0f0:
    ipv4_subnets:
      - 10.110.192.48/30
    ipv6_subnets:
      - fe80::/64
  scion-gateway:
    ipv4_subnets:
      - 192.168.110.0/24
      - 192.168.111.0/24
    ipv6_subnets:
      - fe80::/64
```

## 168980 - Enumerate the PATH Variables

### Synopsis

Enumerates the PATH variable of the current scan user.

### Description

Enumerates the PATH variables of the current scan user.

### Solution

Ensure that directories listed here are in line with corporate policy.

### Risk Factor

None

### Plugin Information

Published: 2022/12/21, Modified: 2024/08/08

### 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
/snap/bin
```

## 35716 - Ethernet Card Manufacturer Detection

### Synopsis

The manufacturer can be identified from the Ethernet OUI.

### Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

### See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

### Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:90:0B:A5:D2:91 : LANNER ELECTRONICS, INC.
00:90:0B:A5:D2:8F : LANNER ELECTRONICS, INC.
00:90:0B:A5:D2:93 : LANNER ELECTRONICS, INC.
00:90:0B:A5:D2:8E : LANNER ELECTRONICS, INC.
00:90:0B:A5:D2:90 : LANNER ELECTRONICS, INC.
00:90:0B:A5:D2:92 : LANNER ELECTRONICS, INC.
00:90:0B:A5:D2:94 : LANNER ELECTRONICS, INC.
00:90:0B:A5:D2:95 : LANNER ELECTRONICS, INC.
```

## 86420 - Ethernet MAC Addresses

### Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

### Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

### Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 00:90:0B:A5:D2:91
  - 00:90:0B:A5:D2:8F
  - 00:90:0B:A5:D2:93
  - 00:90:0B:A5:D2:8E
  - 00:90:0B:A5:D2:90
  - 00:90:0B:A5:D2:92
  - 02:42:C7:7B:2B:AA
  - 00:90:0B:A5:D2:94
  - 00:90:0B:A5:D2:95
```

## 49704 - External URLs

### Synopsis

Links to external sites were gathered.

### Description

Nessus gathered HREF links to external sites by crawling the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/10/04, Modified: 2011/08/19

### Plugin Output

tcp/443/www

```
1 external URL was gathered on this web server :
URL...                                  - Seen on...


https://fonts.gstatic.com               - /ui
```

## 84502 - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

https://tools.ietf.org/html/rfc6797

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information

Published: 2015/07/02, Modified: 2024/08/09

### Plugin Output

tcp/443/www

```
HTTP/1.1 301 Moved Permanently
Alt-Svc: h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000
Content-Length: 38
Content-Type: text/html; charset=utf-8
Date: Mon, 12 Aug 2024 11:50:20 GMT
Location: /ui
Server: Caddy
Connection: close

The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/80/www

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
    INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/443/www

```
Based on tests of each method :

  - HTTP methods CONNECT DELETE GET HEAD OPTIONS PATCH POST PUT TRACE
    are allowed on :

    /
    /ui
```

## 43111 - HTTP Methods Allowed (per directory)

### Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

### Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

### See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

### Plugin Output

tcp/42001/www

```
Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD
    INDEX LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE MOVE NOTIFY
    OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT
    RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE TRACE UNCHECKOUT UNLOCK
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /

  - Invalid/unknown HTTP methods are allowed on :

    /
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

tcp/80/www

```
The remote web server type is :

Caddy
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0931

### Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

### Plugin Output

tcp/443/www

```
The remote web server type is :

Caddy
```

## 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/42001/www

```
The remote web server type is :

Caddy
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

### Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 308 Permanent Redirect

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Connection: close
  Location: https://192.168.112.1/
  Server: Caddy
  Date: Mon, 12 Aug 2024 11:56:59 GMT
  Content-Length: 0

Response Body :
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

### Plugin Output

tcp/443/www

```
Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1
HTTP/2 TLS Support: Yes
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Alt-Svc: h3=":443"; ma=2592000,h3=":443"; ma=2592000,h3=":443"; ma=2592000
  Content-Length: 38
  Content-Type: text/html; charset=utf-8
  Date: Mon, 12 Aug 2024 11:56:59 GMT
  Location: /ui
  Server: Caddy
  Connection: close

Response Body :

<a href="/ui">Moved Permanently</a>.
```

## 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/42001/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

  Server: Caddy
  Date: Mon, 12 Aug 2024 11:56:59 GMT
  Content-Length: 0
  Connection: close

Response Body :
```

## 91634 - HyperText Transfer Protocol (HTTP) Redirect Information

### Synopsis

The remote web server redirects requests to the root directory.

### Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

### Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

### Risk Factor

None

### Plugin Information

Published: 2016/06/16, Modified: 2017/10/12

### Plugin Output

tcp/443/www

```
Request         : https://192.168.112.1/
HTTP response   : HTTP/1.1 301 Moved Permanently
Redirect to     : https://192.168.112.1/ui
Redirect type   : 30x redirect

Final page      : https://192.168.112.1/ui
HTTP response   : HTTP/1.1 200 OK
```

## 171410 - IP Assignment Method Detection

### Synopsis

Enumerates the IP address assignment method(static/dynamic).

### Description

Enumerates the IP address assignment method(static/dynamic).

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/02/14, Modified: 2024/08/08

### Plugin Output

tcp/0

```
+ lo
  + IPv4
    - Address       : 127.0.0.1
      Assign Method : static
  + IPv6
    - Address       : ::1
      Assign Method : static
+ enp2s0f0
  + IPv4
    - Address       : 10.110.192.49
      Assign Method : static
  + IPv6
    - Address       : fe80::290:bff:fea5:d28e
      Assign Method : static
+ enp2s0f1
+ enp2s0f2
+ enp8s0f0
+ enp2s0f3
+ enp8s0f1
+ enp10s0f0
+ wg0
  + IPv4
    - Address       : 198.18.30.3
      Assign Method : static
+ docker0
  + IPv4
    - Address       : 172.17.0.1
      Assign Method : static
+ enp10s0f1
  + IPv4
    - Address       : 192.168.112.1
      Assign Method : static
```

```
  + IPv6
    - Address       : fe80::290:bff:fea5:d295
      Assign Method : static
+ scion-gateway
  + IPv6
    - Address       : fe80::ca8e:c258:f7cb:b9e8
      Assign Method : static
+ i.ABAAAAQAAAAC2
```

## 14788 - IP Protocols Scan

### Synopsis

This plugin detects the protocols understood by the remote IP stack.

### Description

This plugin detects the protocols understood by the remote IP stack.

### See Also

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/09/22, Modified: 2022/08/15

### Plugin Output

tcp/0

```
The following IP protocols are accepted on this host:
1ICMP
2IGMP
4IP
6TCP
17UDP
41IPv6
50ESP
103PIM
112VRRP
136UDPLite
```

## 118237 - JAR File Detection for Linux/UNIX

### Synopsis

Detected JAR files on the host.

### Description

The host contains JAR files, Java Archive files.

Note that this plugin only detects JAR files in commonly used installation directories or a user specified search path.

### See Also

https://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2018/10/22, Modified: 2024/08/08

### Plugin Output

tcp/0

```
JAR files found: 2
  - /usr/share/java/libintl-0.21.jar
  - /var/lib/docker/overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/
usr/share/java/libintl.jar
```

## 151883 - Libgcrypt Installed (Linux/UNIX)

### Synopsis

Libgcrypt is installed on this host.

### Description

Libgcrypt, a cryptography library, was found on the remote host.

### See Also

https://gnupg.org/download/index.html

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/07/21, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 26 installs of Libgcrypt:

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20.3.4
  Version : 1.9.4

  Path    : /lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.9.4

  Path    : /var/lib/docker/overlay2/
ec9ad3c19c7f6f4040226853edaa4ed220bd5c22539cbe766c97b45c319b7d7c/diff/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.4

  Path    : /var/lib/docker/overlay2/
ec9ad3c19c7f6f4040226853edaa4ed220bd5c22539cbe766c97b45c319b7d7c/diff/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.4
  Version : 1.8.4
```

```
  Path    : /var/lib/docker/
overlay2/1ec83b578c77fef6bba72f867d2532c82155d89a5f3047c51f435a81938932cf/diff/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.4

  Path    : /var/lib/docker/
overlay2/1ec83b578c77fef6bba72f867d2532c82155d89a5f3047c51f435a81938932cf/diff/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.4
  Version : 1.8.4

  Path    : /var/lib/docker/
overlay2/80db2826be887e1cd0569da2bcc0cd908df6a6ebb5c8ac92e6189f17b4ba00d2/merged/usr/lib/x86_64-
linux-gnu/libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/80db2826be887e1cd0569da2bcc0cd908df6a6ebb5c8ac92e6189f17b4ba00d2/merged/usr/lib/x86_64-
linux-gnu/libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/V557QCG64WEESUY6CZCKRZEBMM/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/V557QCG64WEESUY6CZCKRZEBMM/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/6LMLXJ66236VHEHQ4INAAYX5WM/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.4

  Path    : /var/lib/docker/overlay2/l/6LMLXJ66236VHEHQ4INAAYX5WM/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.4
  Version : 1.8.4

  Path    : /var/lib/docker/overlay2/l/CN4AZCGU3WBMUEUFOXW7UXQR7Q/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.4

  Path    : /var/lib/docker/overlay2/l/CN4AZCGU3WBMUEUFOXW7UXQR7Q/lib/x86_64-linux-gn [...]
```

## 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
tmpfs                              790M  1.9M  789M   1% /run
/dev/mapper/anapaya--v3--vg-root    49G   21G   26G  44% /
tmpfs                              3.9G     0  3.9G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
overlay                             49G   21G   26G  44% /var/lib/docker/
overlay2/745d88d99c32ea92d4a04bfceb6cdbf8eec6ab927222053d4141c2d99361ff74/merged
overlay                             49G   21G   26G  44% /var/lib/docker/
overlay2/80db2826be887e1cd0569da2bcc0cd908df6a6ebb5c8ac92e6189f17b4ba00d2/merged
overlay                             49G   21G   26G  44% /var/lib/docker/
overlay2/5df41ba671fe5f7f2fa5ac7b492f0618d6a641ec6dca02948ab6b194642b5f87/merged
overlay                             49G   21G   26G  44% /var/lib/docker/
overlay2/449201ff4c2bfc895d6381f1de5c490816e97243f6452b75a4dd4aa52404af90/merged
overlay                             49G   21G   26G  44% /var/lib/docker/overlay2/
b03508299408005aebc0dcb90b1c06e0cb25047c05b62b9bef4609cc8b64efd4/merged
overlay                             49G   21G   26G  44% /var/lib/docker/overlay2/
e90f2d6a9802783c32552768a493b07f39ce939fed034da80fd357844a0d90be/merged
overlay                             49G   21G   26G  44% /var/lib/docker/
overlay2/6a5603561d64d2255dd90b2daea2bc37f041c3e54d733d8a38fb2cdde6cfcb2f/merged
overlay                             49G   21G   26G  44% /var/lib/docker/
overlay2/1158a61343a5a8c9372d4206063b3efa753c1ab8476ba2e79982d6c55c1d8fd0/merged
overlay                             49G   21G   26G  44% /var/lib/docker/overlay2/
c3f65e36566042561f3904172f371e2cf28de5f3434936d96fd39f46e5ed3d14/merged
```

```
overlay                          49G   21G   26G  44% /var/lib/docker/overlay2/
bb40bac61ef3914de394399ae49079785d53aa75eb267833c45e76568af94e39/merged
overlay                          49G   21G   26G  44% /var/lib/docker/overlay2/
b9b3fef9f7011cc465271a0e3b2b5ab346503c94a180699c53a8dbf39677419b/merged


$ lsblk
NAME                      MAJ: [...]
```

## 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: Etc/UTC (UTC, +0000)
Via /etc/timezone: Etc/UTC
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: 2024/03/13

### Plugin Output

tcp/0

```
----------[ User Accounts ]-----------

User         : anapaya
Home folder  : /home/anapaya
Start script : /bin/bash
Groups       : anapaya
               lpadmin
               cdrom
               sambashare
               sudo
               plugdev
               dip
               adm

User         : scion
Home folder  : /home/scion
Start script : /bin/bash
Groups       : scion
               sudo
               adm

User         : prometheus
Home folder  : /
Start script : /bin/false
Groups       : prometheus

----------[ System Accounts ]----------

User         : root
```

```
Home folder  : /root
Start script : /bin/bash
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

U [...]
```

## 45433 - Memory Information (via DMI)

### Synopsis

Information about the remote system's memory devices can be read.

### Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's memory devices, such as the total amount of installed memory.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/06, Modified: 2018/03/29

### Plugin Output

tcp/0

```
Total memory : 8192 MB
```

## 50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

### See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

### Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/443/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

  - https://192.168.112.1/ui
  - https://192.168.112.1/ui/
```

## 50345 - Missing or Permissive X-Frame-Options HTTP Response Header

### Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

### Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

### See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

### Solution

Set a properly configured X-Frame-Options header for all requested resources.

### Risk Factor

None

### Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

### Plugin Output

tcp/443/www

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - https://192.168.112.1/ui
  - https://192.168.112.1/ui/
```

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2005/08/26, Modified: 2024/08/05

### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.8.1
Nessus build : 20004
Plugin feed version : 202408120709
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : Advanced Scan
```

```
Scan policy used : Advanced Scan
Scanner IP : 192.168.110.80
Port scanner(s) : netstat
Port range : 0-65535
Ping RTT : 85.439 ms
Thorough tests : yes
Experimental tests : no
Scan for Unpatched Vulnerabilities : yes
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'scion' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : yes
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : never
Max hosts : 100
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 : 2024/8/12 13:48 CEST
Scan duration : 1573 sec
Scan for malware : yes
```

## 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: 2024/07/24

### 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: 2024/07/24

### Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

## 14272 - Netstat Portscanner (SSH)

### Synopsis

Remote open ports can be enumerated via SSH.

### Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports. If 'netstat' is not available, the plugin will attempt to use 'ss'.

See the section 'plugins options' about configuring this plugin.

Note: This plugin will run on Windows (using netstat.exe) in the event that the target being scanned is localhost.

### See Also

https://en.wikipedia.org/wiki/Netstat

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2004/08/15, Modified: 2024/07/24

### Plugin Output

tcp/443/www

```
Port 443/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: 2024/07/24

### Plugin Output

udp/443

```
Port 443/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: 2024/07/24

### Plugin Output

udp/30041

```
Port 30041/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: 2024/07/24

### Plugin Output

udp/30042

```
Port 30042/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: 2024/07/24

### Plugin Output

tcp/30252

```
Port 30252/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: 2024/07/24

### Plugin Output

tcp/42001/www

```
Port 42001/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: 2024/07/24

### Plugin Output

udp/51021

```
Port 51021/udp was found to be open
```

## 33851 - Network daemons not managed by the package system

### Synopsis

Some daemon processes on the remote host are associated with programs that have been installed manually.

### Description

Some daemon processes on the remote host are associated with programs that have been installed manually.

System administration best practice dictates that an operating system's native package management tools be used to manage software installation, updates, and removal whenever possible.

### Solution

Use packages supplied by the operating system vendor whenever possible.

And make sure that manual software installation agrees with your organization's acceptable use and security policies.

### Risk Factor

None

### Plugin Information

Published: 2008/08/08, Modified: 2024/03/06

### Plugin Output

tcp/0

```
The following running daemons are not managed by dpkg :

/usr/local/bin/appliance
/usr/local/bin/debugscraper
```

## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2003/12/09, Modified: 2024/06/19

### Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 5.15.0-116-generic on Ubuntu 22.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 5.15.0-116-generic on Ubuntu 22.04
```

## 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: 2024/03/19

### Plugin Output

tcp/0

```
It was possible to log into the remote host via SSH using 'publickey' authentication.

The output of "uname -a" is :
Linux s01-chlau1-arma 5.15.0-116-generic #126-Ubuntu SMP Mon Jul 1 10:14:24 UTC 2024 x86_64 x86_64
 x86_64 GNU/Linux

Local checks have been enabled for this host.
The remote Debian system is :
bookworm/sid

This is a Ubuntu system

OS Security Patch Assessment is available for this host.
Runtime : 43.680155 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.

Account  : scion
Protocol : SSH
```

## 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: 2024/08/08

### Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 8.9p1
Banner  : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
```

## 66334 - Patch Report

### Synopsis

The remote host is missing several patches.

### Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

### Solution

Install the patches listed below.

### Risk Factor

None

### Plugin Information

Published: 2013/07/08, Modified: 2024/07/15

### Plugin Output

tcp/0

```
. You need to take the following 15 actions :


[ Curl 7.32.0 < 8.9.1 DoS (CVE-2024-7264) (205023) ]

+ Action to take : Upgrade Curl to version 8.9.1 or later

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : shadow vulnerability
 (USN-6640-1) (190598) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Kerberos
 vulnerabilities (USN-6947-1) (205195) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).
```

```
[ Ubuntu 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)
 (185568) ]

+ Action to take : Update the affected traceroute package.


[ Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : pip vulnerabilities
 (USN-6473-2) (185739) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).


[ Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GLib vulnerability (USN-6768-1) (195216) ]

+ Action to take : Update the affected packages.


[ Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : OpenSSL vulnerabilities (USN-6937-1) (204924) ]

+ Action to take : Update the affected packages.

+Impact : Taking this action will resolve 4 different vulnerabilities (CVEs).


[ Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : curl vulnerability (USN-6944-1) (204989) ]

+ Action to take : Update the affected packages.


[ Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6923-1) (204913) ]

+ Action to take : Update the affected kernel package.

+Impact : Taking this action will resolve 6 different vulnerabilities (CVEs).


[ Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6950-1) (205227) ]

+ Action to take : Update the affected kernel package.


[ Ubuntu 20.04 LTS / 22.04 LTS : OpenLDAP vulnerability (USN-6616-1) (1 [...]
```

## 45432 - Processor Information (via DMI)

### Synopsis

Nessus was able to read information about the remote system's processor.

### Description

Nessus was able to retrieve information about the remote system's hardware, such as its processor type, by using the SMBIOS (aka DMI) interface.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2010/04/06, Modified: 2016/02/25

### Plugin Output

tcp/0

```
Nessus detected 1 processor :

Current Speed   : 2200 MHz
Version         : Intel(R) Atom(TM) CPU C3558 @ 2.20GHz
Manufacturer    : Intel(R) Corporation
External Clock  : 100 MHz
Status          : Populated, Enabled
Family          : Pentium 4
Type            : Central Processor
```

## 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   : 897
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/443

```
Process ID   : 239110
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 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/30041

```
Process ID   : 241025
Executable   : /app/scion-all
Command line : /app/scion-all dispatcher --config /share/conf/dispatcher.toml
```

## 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/30042

```
Process ID   : 240906
Executable   : /usr/bin/vpp
Command line : /usr/bin/vpp -c /share/conf/dataplane.conf
```

## 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/30252

```
Process ID   : 240671
Executable   : /app/scion-all
Command line : /app/scion-all control --config /share/conf/control.toml
```

## 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/42001/www

```
Process ID   : 239110
Executable   : /usr/bin/caddy
Command line : /usr/bin/caddy run --environ --config /etc/caddy/config.json --resume
```

## 174788 - SQLite Local Detection (Linux)

### Synopsis

The remote Linux host has SQLite Database software installed.

### Description

Version information for SQLite was retrieved from the remote host. SQLite is an embedded database written in C.

- To discover instances of SQLite that are not in PATH, or installed via a package manager, 'Perform thorough tests' setting must be enabled.

### See Also

https://www.sqlite.org/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2023/04/26, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Path    : /usr/share/bash-completion/completions/sqlite3
Version : unknown
```

## 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: 2017/08/28

### Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256
  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group14-sha256
  diffie-hellman-group16-sha512
  diffie-hellman-group18-sha512
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521
  kex-strict-s-v00@openssh.com
  sntrup761x25519-sha512@openssh.com

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  rsa-sha2-256
  rsa-sha2-512
  ssh-ed25519

The server supports the following options for encryption_algorithms_client_to_server :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
```

```
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

  aes128-ctr
  aes128-gcm@openssh.com
  aes192-ctr
  aes256-ctr
  aes256-gcm@openssh.com
  chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-sha1
  hmac-sha1-etm@openssh.com
  hmac-sha2-256
  hmac-sha2-256-etm@openssh.com
  hmac-sha2-512
  hmac-sha2-512-etm@openssh.com
  umac-128-etm@openssh.com
  umac-128@openssh.com
  umac-64-etm@openssh.com
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@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
```

## 90707 - SSH SCP Protocol Detection

### Synopsis

The remote host supports the SCP protocol over SSH.

### Description

The remote host supports the Secure Copy (SCP) protocol over SSH.

### See Also

https://en.wikipedia.org/wiki/Secure_copy

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/04/26, Modified: 2024/07/24

### Plugin Output

tcp/22/ssh

## 153588 - SSH SHA-1 HMAC Algorithms Enabled

### Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

### Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

### Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are
 supported :

  hmac-sha1
  hmac-sha1-etm@openssh.com
```

## 10267 - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

### Solution

n/a

### Risk Factor

None

### References

XREF IAVT:0001-T-0933

### Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

### Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
SSH supported authentication : publickey
```

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/01, Modified: 2023/07/10

### Plugin Output

tcp/443/www

```
This port supports TLSv1.3/TLSv1.2.
```

## 83298 - SSL Certificate Chain Contains Certificates Expiring Soon

### Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

### Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

### Solution

Renew any soon to expire SSL certificates.

### Risk Factor

None

### Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

### Plugin Output

tcp/443/www

```
The following soon to expire certificates were part of the
certificate chain sent by the remote host :

|-Subject   : CN=Caddy Local Authority - ECC Intermediate
|-Not After : Aug 16 07:33:44 2024 GMT

|-Subject   :
|-Not After : Aug 12 23:18:59 2024 GMT
```

## 42981 - SSL Certificate Expiry - Future Expiry

### Synopsis

The SSL certificate associated with the remote service will expire soon.

### Description

The SSL certificate associated with the remote service will expire soon.

### Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

### Risk Factor

None

### Plugin Information

Published: 2009/12/02, Modified: 2020/09/04

### Plugin Output

tcp/443/www

```
The SSL certificate will expire within 60 days, at
Aug 12 23:18:59 2024 GMT :

  Subject          : n/a
  Issuer           : CN=Caddy Local Authority - ECC Intermediate
  Not valid before : Aug 12 11:18:59 2024 GMT
  Not valid after  : Aug 12 23:18:59 2024 GMT
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 7F 6F 05 17 68 33 94 DF 63 DC 61 16 F5 67 8B F6

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:18:59 2024 GMT
Not Valid After: Aug 12 23:18:59 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 4B BD B2 FF E0 EF 7D B5 90 C8 B9 26 94 D9 6A 82 5E 06 31 38
              FC 7D FD E3 7B 16 E6 3B 4B 41 D1 E9
Public Key Y: 69 CA 55 CC 1A 4C D8 15 10 FC 87 D1 5F 92 51 29 17 EC B0 CE
              F7 1C 0F 32 96 B3 F9 15 92 C7 EE 50

Signature Length: 72 bytes / 576 bits
Signature: 00 30 46 02 21 00 8C A3 BD FB BD 2A 12 B8 C9 0C A3 3C FA 8E
           B0 97 DF 42 82 2F E7 7B B3 07 5C A3 C1 26 B8 0F 84 B9 02 21
           00 F6 5B D9 92 36 B4 9E DF 66 E2 43 32 11 3F 6C B9 09 55 21
           84 AF 85 7C 9A FF A9 3E 68 99 A2 45 55
```

```
Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4A 9B 5F 85 7D 4E 9E B5 7E E2 B7 6C A3 69 B1 57 BD F0 F9 9A


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 3D 44 BC 03 7C 0D 34 50 41 60 CD 61 E1 56 64 73 6A 07 27 85


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1


Fingerprints :

SHA-256 Fingerprint: 11 51 BB 5E 8F D9 BA AE D5 1F 2E FD D6 ED FD 72 23 78 6C C6
                     80 59 83 2D 96 E5 C4 F1 E0 15 A7 95
SHA-1 Fingerprint: C5 0C E9 CC 8F 13 0F FC D8 4F BE E5 26 6A 70 BE 76 24 5C 4C
MD5 Fingerprint: 72 3B C2 61 5F 5F 1C AE 3D B8 48 04 03 37 8C 6D


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV6gAwIBAgIQf28FF2gzlN9j3GEW9WeL9jAKBggqhkjOPQQDAjAzMTEwLwYDVQQDEyhDYWRkeSBMb2NhbCBBdXRob3JpdHkgLSBFQ0MgSW
 [...]
```

## 159544 - SSL Certificate with no Common Name

### Synopsis

Checks for an SSL certificate with no Common Name

### Description

The remote system is providing an SSL/TLS certificate without a subject common name field. While this is not required in all cases, it is recommended to ensure broad compatibility.

### See Also

https://datatracker.ietf.org/doc/html/rfc5280#section-4.1.2.6

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/06, Modified: 2022/11/30

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 7F 6F 05 17 68 33 94 DF 63 DC 61 16 F5 67 8B F6

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:18:59 2024 GMT
Not Valid After: Aug 12 23:18:59 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 4B BD B2 FF E0 EF 7D B5 90 C8 B9 26 94 D9 6A 82 5E 06 31 38
              FC 7D FD E3 7B 16 E6 3B 4B 41 D1 E9
Public Key Y: 69 CA 55 CC 1A 4C D8 15 10 FC 87 D1 5F 92 51 29 17 EC B0 CE
```

```
               F7 1C 0F 32 96 B3 F9 15 92 C7 EE 50

Signature Length: 72 bytes / 576 bits
Signature: 00 30 46 02 21 00 8C A3 BD FB BD 2A 12 B8 C9 0C A3 3C FA 8E
           B0 97 DF 42 82 2F E7 7B B3 07 5C A3 C1 26 B8 0F 84 B9 02 21
           00 F6 5B D9 92 36 B4 9E DF 66 E2 43 32 11 3F 6C B9 09 55 21
           84 AF 85 7C 9A FF A9 3E 68 99 A2 45 55

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4A 9B 5F 85 7D 4E 9E B5 7E E2 B7 6C A3 69 B1 57 BD F0 F9 9A


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 3D 44 BC 03 7C 0D 34 50 41 60 CD 61 E1 56 64 73 6A 07 27 85


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV6gAwIBAgIQf28FF2gzlN9j3GEW9WeL9jAKBggqhkjOPQQDAjAzMTEwLwYDVQQDEyhDYWRkeSBMb2NhbCBBdXRob3JpdHkgLSBFQ0MgSW
g7321kMi5JpTZaoJeBjE4/H3943sW5jtLQdHpacpVzBpM2BUQ/
IfRX5JRKRfssM73HA8ylrP5FZLH7lCjgYYwgYMwDgYDVR0PAQH/
BAQDAgeAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUSptfhX1OnrV+4rdso2mxV73w
+ZowHwYDVR0jBBgwFoAUPUS8A3wNNFBBYM1h4VZkc2oHJ4UwEgYDVR0RAQH/BAgwBocE [...]
```

## 159545 - SSL Certificate with no Subject

### Synopsis

Checks for an SSL certificate with no Subject

### Description

The remote system is providing an SSL/TLS certificate without a subject field. While this is not required in all cases, it is recommended to ensure broad compatibility.

### See Also

https://datatracker.ietf.org/doc/html/rfc5280#section-4.1.2.6

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2022/04/06, Modified: 2022/11/30

### Plugin Output

tcp/443/www

```
Subject Name:


Issuer Name:

Common Name: Caddy Local Authority - ECC Intermediate

Serial Number: 7F 6F 05 17 68 33 94 DF 63 DC 61 16 F5 67 8B F6

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Aug 12 11:18:59 2024 GMT
Not Valid After: Aug 12 23:18:59 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 4B BD B2 FF E0 EF 7D B5 90 C8 B9 26 94 D9 6A 82 5E 06 31 38
              FC 7D FD E3 7B 16 E6 3B 4B 41 D1 E9
Public Key Y: 69 CA 55 CC 1A 4C D8 15 10 FC 87 D1 5F 92 51 29 17 EC B0 CE
```

```
              F7 1C 0F 32 96 B3 F9 15 92 C7 EE 50

Signature Length: 72 bytes / 576 bits
Signature: 00 30 46 02 21 00 8C A3 BD FB BD 2A 12 B8 C9 0C A3 3C FA 8E
           B0 97 DF 42 82 2F E7 7B B3 07 5C A3 C1 26 B8 0F 84 B9 02 21
           00 F6 5B D9 92 36 B4 9E DF 66 E2 43 32 11 3F 6C B9 09 55 21
           84 AF 85 7C 9A FF A9 3E 68 99 A2 45 55

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature


Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)


Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: 4A 9B 5F 85 7D 4E 9E B5 7E E2 B7 6C A3 69 B1 57 BD F0 F9 9A


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 3D 44 BC 03 7C 0D 34 50 41 60 CD 61 E1 56 64 73 6A 07 27 85


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV6gAwIBAgIQf28FF2gzlN9j3GEW9WeL9jAKBggqhkjOPQQDAjAzMTEwLwYDVQQDEyhDYWRkeSBMb2NhbCBBdXRob3JpdHkgLSBFQ0MgSW
g7321kMi5JpTZaoJeBjE4/H3943sW5jtLQdHpacpVzBpM2BUQ/
IfRX5JRKRfssM73HA8ylrP5FZLH7lCjgYYwgYMwDgYDVR0PAQH/
BAQDAgeAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUSptfhX1OnrV+4rdso2mxV73w
+ZowHwYDVR0jBBgwFoAUPUS8A3wNNFBBYM1h4VZkc2oHJ4UwEgYDVR0RAQH/BAgwBocE [...]
```

## 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/443/www

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    TLS_AES_128_GCM_SHA256        0x13, 0x01        -             -        AES-GCM(128)
 AEAD
    TLS_AES_256_GCM_SHA384        0x13, 0x02        -             -        AES-GCM(256)
 AEAD
    TLS_CHACHA20_POLY1305_SHA256  0x13, 0x03        -             -        ChaCha20-Poly1305(256)
 AEAD


SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption              MAC
    ----------------------        ----------        ---           ----     ---------------------   ---
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B        ECDH          ECDSA    AES-GCM(128)
 SHA256
```

```
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C       ECDH           ECDSA    AES-GCM(256)
 SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9       ECDH           ECDSA    ChaCha20-Poly1305(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

## 57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

### Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

### Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

### See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

### Plugin Output

tcp/443/www

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    ECDHE-ECDSA-AES128-SHA256     0xC0, 0x2B        ECDH          ECDSA    AES-GCM(128)
 SHA256
    ECDHE-ECDSA-AES256-SHA384     0xC0, 0x2C        ECDH          ECDSA    AES-GCM(256)
 SHA384
    ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA9        ECDH          ECDSA    ChaCha20-Poly1305(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
```

```
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/80/www

```
A web server is running on this port.
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/08/19, Modified: 2024/03/26

### Plugin Output

tcp/443/www

```
A TLSv1.2 server answered on this port.
```

tcp/443/www

```
A web server is running on this port through TLSv1.2.
```

## 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/42001/www

```
A web server is running on this port.
```

## 11153 - Service Detection (HELP Request)

### Synopsis

The remote service could be identified.

### Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP'

request.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2018/11/26

### 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: 2022/09/06

### Plugin Output

tcp/0

```
Here is the list of packages installed on the remote Debian Linux system :

  ii   adduser  3.118ubuntu5  all  add and remove users and groups
  ii   amd64-microcode  3.20191218.1ubuntu2.2  amd64  Processor microcode firmware for AMD CPUs
  ii   anapaya-appliance-installer  1.3.0  amd64  The installer of the Anapaya appliance.
  ii   anapaya-system-config  1.4.0  amd64  System configuration for Anapaya appliances.
  ii   apparmor  3.0.4-2ubuntu2.3  amd64  user-space parser utility for AppArmor
  ii   apt  2.4.12  amd64  commandline package manager
  ii   apt-transport-https  2.4.12  all  transitional package for https support
  ii   apt-utils  2.4.12  amd64  package management related utility programs
  ii   base-files  12ubuntu4.6  amd64  Debian base system miscellaneous files
  ii   base-passwd  3.5.52build1  amd64  Debian base system master password and group files
  ii   bash  5.1-6ubuntu1.1  amd64  GNU Bourne Again SHell
  ii   bash-completion  1:2.11-5ubuntu1  all  programmable completion for the bash shell
  ii   bind9-dnsutils  1:9.18.28-0ubuntu0.22.04.1  amd64  Clients provided with BIND 9
  ii   bind9-host  1:9.18.28-0ubuntu0.22.04.1  amd64  DNS Lookup Utility
  ii   bind9-libs  1:9.18.28-0ubuntu0.22.04.1  amd64  Shared Libraries used by BIND 9
  ii   binutils  2.38-4ubuntu2.6  amd64  GNU assembler, linker and binary utilities
  ii   binutils-common  2.38-4ubuntu2.6  amd64  Common files for the GNU assembler, linker and
 binary utilities
  ii   binutils-x86-64-linux-gnu  2.38-4ubuntu2.6  amd64  GNU binary utilities, for x86-64-linux-gnu
 target
```

```
  ii   bsdextrautils  2.37.2-4ubuntu3.4  amd64  extra utilities from 4.4BSD-Lite
  ii   bsdutils  1:2.37.2-4ubuntu3.4  amd64  basic utilities from 4.4BSD-Lite
  ii   busybox-initramfs  1:1.30.1-7ubuntu3  amd64  Standalone shell setup for initramfs
  ii   busybox-static  1:1.30.1-7ubuntu3  amd64  Standalone rescue shell with tons of builtin
utilities
  ii   bzip2  1.0.8-5build1  amd64  high-quality block-sorting file compressor - utilities
  ii   ca-certificates  2 [...]
```

## 35351 - System Information Enumeration (via DMI)

### Synopsis

Information about the remote system's hardware can be read.

### Description

Using the SMBIOS (aka DMI) interface, it was possible to retrieve information about the remote system's hardware, such as its product name and serial number.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2009/01/12, Modified: 2024/07/29

### Plugin Output

tcp/0

```
Chassis Information
  Serial Number : LR202108020621
  Version       : Default string
  Manufacturer  : Default string
  Lock          : Not Present
  Type          : Low Profile Desktop

System Information
  Serial Number : LR202108020621
  Version       : V1.0
  Manufacturer  : Lanner Electronics Inc.
  Product Name  : NCA-1515B
  Family        : Default string
```

## 25220 - TCP/IP Timestamps Supported

### Synopsis

The remote service implements TCP timestamps.

### Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

### See Also

http://www.ietf.org/rfc/rfc1323.txt

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2007/05/16, Modified: 2023/10/17

### Plugin Output

tcp/0

## 136318 - TLS Version 1.2 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.2.

### See Also

https://tools.ietf.org/html/rfc5246

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

### Plugin Output

tcp/443/www

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

## 138330 - TLS Version 1.3 Protocol Detection

### Synopsis

The remote service encrypts traffic using a version of TLS.

### Description

The remote service accepts connections encrypted using TLS 1.3.

### See Also

https://tools.ietf.org/html/rfc8446

### Solution

N/A

### Risk Factor

None

### Plugin Information

Published: 2020/07/09, Modified: 2023/12/13

### Plugin Output

tcp/443/www

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

## 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/22/ssh

```
Nessus was able to log into the remote host with no privilege or access
problems via the following :

User:       'scion'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo
```

## 141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

### Synopsis

Valid credentials were provided for an available authentication protocol.

### Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2020/10/15, Modified: 2024/03/25

### Plugin Output

tcp/22/ssh

```
Nessus was able to log in to the remote host via the following :

User:       'scion'
Port:       22
Proto:      SSH
Method:     publickey
Escalation: sudo
```

## 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  5.15.0-116-gener Wed Jul 24 12:56   still running
reboot   system boot  5.15.0-100-gener Tue Jul 16 14:23 - 12:56 (7+22:32)

wtmp begins Thu Jul 11 06:18:28 2024
```

## 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 192.168.110.80 to 192.168.112.1 :
192.168.110.80
192.168.110.1
?
192.168.112.1

Hop Count: 4
```

## 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.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://xz.tukaani.org/xz-utils/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/03/29, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 20 installs of XZ Utils:

  Path           : /var/lib/docker/
overlay2/78c25587e64b4df48912910324d9db53d2f6df585e6aa71467071cf20acdf688/diff/usr/lib/
liblzma.so.5.2.5
  Version        : 5.2.5
```

```
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/0a0124157fa6efaf256d46f48211edf0593276aa6710f9e9c0268674f0d00086/diff/usr/lib/
liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path    : /var/lib/docker/overlay2/
e90f2d6a9802783c32552768a493b07f39ce939fed034da80fd357844a0d90be/merged/bin/xz
  Version : unknown

  Path           : /var/lib/docker/
overlay2/80db2826be887e1cd0569da2bcc0cd908df6a6ebb5c8ac92e6189f17b4ba00d2/merged/lib/x86_64-linux-
gnu/liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/1c3a6bc1043c947a6318d1e1052a2657d38d8bc5eecbfead5dca5374dc7faca5/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.4
  Version        : 5.2.4
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/1ec83b578c77fef6bba72f867d2532c82155d89a5f3047c51f435a81938932cf/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.4
  Version        : 5.2.4
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/usr/bin/xz
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File contents

  Path           : /var/lib/docker/overlay2/
d2e35fc435eb957b6b10fe04c68382701151d45cb670e2e3dc16e6d5cc9c719c/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version        : 5.2.5
  Confidence     : Medium
  Version Source : File name

  Path           : /var/lib/docker/
overlay2/1eccf5fa4d23f4e56c1c190711d470fcdcf1ca38f99d3b8342a4c0b878ca50de/diff/usr/bin/xz
  Version        : 5.2.4
  Confidence     : Medium
  Version Source : File contents

  Path    : /var/lib/docker/overlay2/528b0bf74837aa7594b022dcaf26c51a11fedd [...]
```

## 183197 - Ubuntu 22.04 ESM : iperf3 vulnerability (USN-6431-3)

### Synopsis

The remote Ubuntu host is missing a security update.

### Description

The remote Ubuntu 22.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-6431-3 advisory.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### See Also

https://ubuntu.com/security/notices/USN-6431-3

### Solution

Update the affected iperf3, libiperf-dev and / or libiperf0 packages.

### Risk Factor

None

### References

| | |
|---|---|
| XREF | USN:6431-3 |

### Plugin Information

Published: 2023/10/16, Modified: 2023/10/16

### Plugin Output

tcp/0

```
  - Installed package : iperf3_3.9-1+deb11u1build0.22.04.1
  - Fixed package     : iperf3_3.9-1+deb11u1ubuntu0.1~esm1

  - Installed package : libiperf0_3.9-1+deb11u1build0.22.04.1
  - Fixed package     : libiperf0_3.9-1+deb11u1ubuntu0.1~esm1


NOTE: The fixed ESM packages referenced in this plugin requires a
subscription to Ubuntu Pro to enable the ESM repositories.
```

## 198218 - Ubuntu Pro Subscription Detection

### Synopsis

The remote Ubuntu host has an active Ubuntu Pro subscription.

### Description

The remote Ubuntu host has an active Ubuntu Pro subscription.

### See Also

https://documentation.ubuntu.com/pro/

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2024/05/31, Modified: 2024/07/05

### Plugin Output

tcp/0

```
This machine is NOT attached to an Ubuntu Pro subscription. However, it may have previously been
 attached.

The following details were gathered from /var/lib/ubuntu-advantage/status.json:
```

## 83303 - Unix / Linux - Local Users Information : Passwords Never Expire

### Synopsis

At least one local user has a password that never expires.

### Description

Using the supplied credentials, Nessus was able to list local users that are enabled and whose passwords never expire.

### Solution

Allow or require users to change their passwords regularly.

### Risk Factor

None

### Plugin Information

Published: 2015/05/10, Modified: 2023/11/27

### Plugin Output

tcp/0

```
Nessus found the following unlocked users with passwords that do not expire :
  - root
  - anapaya
  - scion
```

## 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  0.3  0.1 167436 12112 ?        Ss   Jul24  87:45 /sbin/init noquiet nosplash nofb
root           2  0.0  0.0      0     0 ?        S    Jul24   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Jul24   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Jul24   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   Jul24   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   Jul24   0:00 [netns]
root           8  0.0  0.0      0     0 ?        I<   Jul24   0:00 [kworker/0:0H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   Jul24   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        S    Jul24   0:00 [rcu_tasks_rude_]
root          12  0.0  0.0      0     0 ?        S    Jul24   0:00 [rcu_tasks_trace]
root          13  0.0  0.0      0     0 ?        S    Jul24   1:53 [ksoftirqd/0]
root          14  0.1  0.0      0     0 ?        I    Jul24  32:27 [rcu_sched]
root          15  0.0  0.0      0     0 ?        S    Jul24   0:03 [migration/0]
root          16  0.0  0.0      0     0 ?        S    Jul24   0:00 [idle_inject/0]
root          18  0.0  0.0      0     0 ?        S    Jul24   0:00 [cpuhp/0]
root          19  0.0  0.0      0     0 ?        S    Jul24   0:00 [cpuhp/1]
root          20  0.0  0.0      0     0 ?        S    Jul24   0:00 [idle_inject/1]
root          21  0.0  0.0      0     0 ?        S    Jul24   0:03 [migration/1]
root          22  0.0  0.0      0     0 ?        S    Jul24   1:22 [ksoftirqd/1]
root          24  0.0  0.0      0     0 ?        I<   Jul24   0:00 [kworker/1:0H-events_highpri]
root          25  0.0  0.0      0     0 ?        S    Jul24   0:00 [cpuhp/2]
root          26  0.0  0.0      0     0 ?        S    Jul24   0:00 [idle_inject/2]
root          27  0.0  0.0      0     0 ?        S    Jul24   0:03 [migration/2]
root          28  0.0  0.0      0     0 ?        S    Jul24   0:11 [ksoft [...]
```

## 152743 - Unix Software Discovery Commands Not Available

### Synopsis

Nessus was able to log in to the remote host using the provided credentials, but encountered difficulty running commands used to find unmanaged software.

### Description

Nessus found problems running commands on the target host which are used to find software that is not managed by the operating system.

Details of the issues encountered are reported by this plugin.

Failure to properly execute commands used to find and characterize unmanaged software on the target host can lead to scans that do not report known vulnerabilities. There may be little in the scan results of unmanaged software plugins to indicate the missing availability of the source commands except audit trail messages.

Commands used to find unmanaged software installations might fail for a variety of reasons, including:

* Inadequate scan user permissions,

* Failed privilege escalation,

* Intermittent network disruption, or

* Missing or corrupt executables on the target host.

Please address the issues reported here and redo the scan.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2021/08/23, Modified: 2021/08/23

### Plugin Output

tcp/0

```
Failures in commands used to assess Unix software:

  unzip -v                    :
    sh: 1: unzip: not found


Account  : scion
Protocol : SSH
```

## 11154 - Unknown Service Detection: Banner Retrieval

### Synopsis

There is an unknown service running on the remote host.

### Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

### Plugin Output

tcp/30252

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

  Port    : 30252
  Type    : spontaneous
  Banner :
0x00:  00 00 0C 04 00 00 00 00 00 00 05 00 00 40 00 00    .............@..
          0x10:  03 00 00 00 80                                        .....


Nessus detected the following process listening on this port :

/app/scion-all
```

## 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: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 2 installs of Vim:

  Path    : /usr/bin/vim.tiny
  Version : 8.2

  Path    : /usr/bin/vim.basic
  Version : 8.2
```

## 91815 - Web Application Sitemap

### Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

### Description

The remote web server contains linkable content that can be used to gather information about a target.

### See Also

http://www.nessus.org/u?5496c8d9

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

### Plugin Output

tcp/443/www

```
The following sitemap was created from crawling linkable content on the target host :

  - https://192.168.112.1/ui
  - https://192.168.112.1/ui/
  - https://192.168.112.1/ui/favicon.ico
  - https://192.168.112.1/ui/styles.f099f610cfe9907e.css

Attached is a copy of the sitemap file.
```

## 91815 - Web Application Sitemap

### Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

### Description

The remote web server contains linkable content that can be used to gather information about a target.

### See Also

http://www.nessus.org/u?5496c8d9

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

### Plugin Output

tcp/42001/www

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.112.1:42001/

Attached is a copy of the sitemap file.
```

## 10386 - Web Server No 404 Error Code Check

### Synopsis

The remote web server does not return 404 error codes.

### Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

### Solution

n/a

### Risk Factor

None

### Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

### Plugin Output

tcp/42001/www

```
Unfortunately, Nessus has been unable to find a way to recognize this
page so some CGI-related checks have been disabled.
```

## 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.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: 2023/10/10, Modified: 2024/08/08

### Plugin Output

tcp/0

```
Nessus detected 5 installs of libcurl:

  Path    : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/lib/x86_64-linux-
gnu/libcurl.so.4.5.0
  Version : 7.64.0

  Path    : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libcurl.so.4.5.0
  Version : 7.64.0
```

```
  Path    : /var/lib/docker/
overlay2/121ad0592b404cd784e8de1bb8896462fdbee25e117e116dcb8e1deaee5ffa68/diff/usr/lib/x86_64-linux-
gnu/libcurl-gnutls.so.4.5.0
  Version : 7.64.0

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.7.0
  Version            : 7.81.0
  Associated Package : libcurl4 7.81.0-1ubuntu1.16
  Managed by OS      : True

  Path               : /usr/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.7.0
  Version            : 7.81.0
  Associated Package : libcurl3-gnutls 7.81.0-1ubuntu1.16
  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: 2024/08/08

### Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/sbin/nginx
  Version          : 1.19.9
  Detection Method : Binary Located via Search
  Full Version     : 1.19.9
  Nginx Plus       : False
```

# appliance-cron.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# control-64-2_0_2b.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# control-64-2_0_2c.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# control-64-2_0_2d.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# daemon-64-2_0_2b.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# daemon-64-2_0_2c.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# daemon-64-2_0_2d.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# dataplane-control.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# dataplane.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# dispatcher.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# gateway.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# node-exporter.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# promtail.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# router.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities

# telemetry.docker.container


## Host Information

| | |
|---|---|
| IP: | 192.168.112.1 |
| MAC Address: | 00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 02:42:C7:7B:2B:AA 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95 |
| OS: | Linux Kernel 5.15.0-116-generic on Ubuntu 22.04 |

## Vulnerabilities