tenable® Nessus

Advanced Scan

Report generated by Nessus™ Wed, 26 Jun 2024 11:13:37 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.110.1

153	168	260	2	111
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jun 26 10:47:32 2024
End time:	Wed Jun 26 11:09:02 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

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

7.7

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1l
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1l
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1o
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1o
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  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

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             : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
```

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1p
```

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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.5
```

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                                      : /snap/core20/1974/usr/bin/openssl
  Installed version                         : 1.1.1f
  Security End of Life                      : September 11, 2023
  Time since Security End of Life (Est.)    : >= 6 months
```

tcp/0

```
  Path                                    : /snap/core20/1974/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Installed version                       : 1.1.1f
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Installed version                       : 1.1.1f
  Security End of Life                    : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                    : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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
```

194474 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1)

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 / 24.04 LTS. host has a package installed that is affected by a vulnerability as referenced in the USN-6756-1 advisory.

- less through 653 allows OS command execution via a newline character in the name of a file, because quoting is mishandled in filename.c. Exploitation typically requires use with attacker-controlled file names, such as the files extracted from an untrusted archive. Exploitation also requires the LESSOPEN environment variable, but this is set by default in many common cases. (CVE-2024-32487)

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-6756-1

Solution

Update the affected less package.

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

7.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-32487
XREF	USN:6756-1

Plugin Information

Published: 2024/04/29, Modified: 2024/04/29

Plugin Output

tcp/0

```
  - Installed package : less_590-1ubuntu0.22.04.1
  - Fixed package     : less_590-1ubuntu0.22.04.3
```

193362 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1)

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-6736-1 advisory.

- inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9840)

- inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9841)

- zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. (CVE-2018-25032)

- zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference). (CVE-2022-37434)

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-6736-1

Solution

Update the affected klibc-utils, libklibc and / or libklibc-dev 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

6.7

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

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

References

CVE	CVE-2016-9840
CVE	CVE-2016-9841
CVE	CVE-2018-25032
CVE	CVE-2022-37434
XREF	USN:6736-1

Plugin Information

Published: 2024/04/16, Modified: 2024/04/16

Plugin Output

tcp/0

```
  - Installed package : klibc-utils_2.0.10-4
  - Fixed package     : klibc-utils_2.0.10-4ubuntu0.1

  - Installed package : libklibc_2.0.10-4
  - Fixed package     : libklibc_2.0.10-4ubuntu0.1
```

191066 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : less vulnerability (USN-6664-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 host has a package installed that is affected by a vulnerability as referenced in the USN-6664-1 advisory.

- close_altfile in filename.c in less before 606 omits shell_quote calls for LESSCLOSE. (CVE-2022-48624)

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-6664-1

Solution

Update the affected less 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

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-2022-48624
XREF	USN:6664-1

Plugin Information

Published: 2024/02/27, Modified: 2024/03/11

Plugin Output

tcp/0

```
  - Installed package : less_590-1ubuntu0.22.04.1
  - Fixed package     : less_590-1ubuntu0.22.04.2
```

187105 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : OpenSSH vulnerabilities (USN-6560-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6560-1 advisory.

- ssh-add in OpenSSH before 9.3 adds smartcard keys to ssh-agent without the intended per-hop destination constraints. The earliest affected version is 8.9. (CVE-2023-28531)

- The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD 1.3.9rc1, ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust; and there could be effects on Bitvise SSH through 9.31. (CVE-2023-48795)

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-6560-1

Solution

Update the affected packages.

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

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-2023-28531
CVE	CVE-2023-48795
XREF	IAVA:2023-A-0152-S
XREF	USN:6560-1
XREF	IAVA:2023-A-0703

Plugin Information

Published: 2023/12/19, Modified: 2023/12/22

Plugin Output

tcp/0

```
  - Installed package : openssh-client_1:8.9p1-3ubuntu0.3
  - Fixed package     : openssh-client_1:8.9p1-3ubuntu0.5

  - Installed package : openssh-server_1:8.9p1-3ubuntu0.3
  - Fixed package     : openssh-server_1:8.9p1-3ubuntu0.5

  - Installed package : openssh-sftp-server_1:8.9p1-3ubuntu0.3
  - Fixed package     : openssh-sftp-server_1:8.9p1-3ubuntu0.5
```

186300 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Perl vulnerabilities (USN-6517-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6517-1 advisory.

- In Perl 5.34.0, function S_find_uninit_var in sv.c has a stack-based crash that can lead to remote code execution or local privilege escalation. (CVE-2022-48522)

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-6517-1

Solution

Update the affected packages.

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

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)

References

CVE	CVE-2022-48522
CVE	CVE-2023-47038
XREF	USN:6517-1

Plugin Information

Published: 2023/11/27, Modified: 2023/11/27

Plugin Output

tcp/0

```
  - Installed package : libperl5.34_5.34.0-3ubuntu1.2
  - Fixed package     : libperl5.34_5.34.0-3ubuntu1.3

  - Installed package : perl_5.34.0-3ubuntu1.2
  - Fixed package     : perl_5.34.0-3ubuntu1.3

  - Installed package : perl-base_5.34.0-3ubuntu1.2
  - Fixed package     : perl-base_5.34.0-3ubuntu1.3

  - Installed package : perl-modules-5.34_5.34.0-3ubuntu1.2
  - Fixed package     : perl-modules-5.34_5.34.0-3ubuntu1.3
```

198042 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Git vulnerabilities (USN-6793-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6793-1 advisory.

It was discovered that Git incorrectly handled certain submodules. An attacker could possibly use this issue to execute arbitrary code. This issue was fixed in Ubuntu 22.04 LTS, Ubuntu 23.10 and Ubuntu 24.04 LTS. (CVE-2024-32002)

It was discovered that Git incorrectly handled certain cloned repositories. An attacker could possibly use this issue to execute arbitrary code. (CVE-2024-32004)

It was discovered that Git incorrectly handled local clones with hardlinked files/directories. An attacker could possibly use this issue to place a specialized repository on their target's local system.

(CVE-2024-32020)

It was discovered that Git incorrectly handled certain symlinks. An attacker could possibly use this issue to impact availability and integrity creating hardlinked arbitrary files into users repository's objects/directory. (CVE-2024-32021)

It was discovered that Git incorrectly handled certain cloned repositories. An attacker could possibly use this issue to execute arbitrary code. (CVE-2024-32465)

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-6793-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.9

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

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

References

CVE	CVE-2024-32002
CVE	CVE-2024-32004
CVE	CVE-2024-32020
CVE	CVE-2024-32021
CVE	CVE-2024-32465
XREF	USN:6793-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : git_1:2.34.1-1ubuntu1.9
  - Fixed package     : git_1:2.34.1-1ubuntu1.11

  - Installed package : git-man_1:2.34.1-1ubuntu1.9
  - Fixed package     : git-man_1:2.34.1-1ubuntu1.11
```

193515 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU C Library vulnerability (USN-6737-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6737-1 advisory.

- The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable. (CVE-2024-2961)

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-6737-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-2961
XREF	USN:6737-1

Plugin Information

Published: 2024/04/18, Modified: 2024/04/19

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.4
  - Fixed package     : libc-bin_2.35-0ubuntu3.7

  - Installed package : libc6_2.35-0ubuntu3.4
  - Fixed package     : libc6_2.35-0ubuntu3.7

  - Installed package : locales_2.35-0ubuntu3.4
  - Fixed package     : locales_2.35-0ubuntu3.7
```

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

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

6.7

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.
```

148402 - OpenSSL 1.1.1 < 1.1.1j Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

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

- The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23841)

- Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash.

OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i).

Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23840)

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?67f25180

http://www.nessus.org/u?78dabcb5

https://www.openssl.org/news/secadv/20210216.txt

https://www.cve.org/CVERecord?id=CVE-2021-23840

https://www.cve.org/CVERecord?id=CVE-2021-23841

Solution

Upgrade to OpenSSL version 1.1.1j 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

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

VPR Score

6.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-23840
CVE	CVE-2021-23841
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/04/09, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1j
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1j
```

tcp/0

```
Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
Reported version : 1.1.1f
Fixed version    : 1.1.1j
```

148125 - OpenSSL 1.1.1 < 1.1.1k Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

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

- The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a purpose has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named purpose values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions 1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k.

OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).

(CVE-2021-3450)

- An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j). (CVE-2021-3449)

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?144c950a

http://www.nessus.org/u?6aafb4b2

https://www.cve.org/CVERecord?id=CVE-2021-3449

https://www.cve.org/CVERecord?id=CVE-2021-3450

https://www.openssl.org/news/secadv/20210325.txt

Solution

Upgrade to OpenSSL version 1.1.1k or later.

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:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

7.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3449
CVE	CVE-2021-3450
XREF	IAVA:2021-A-0149-S
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/03/25, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1k
```

tcp/0

```
Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
Reported version : 1.1.1f
Fixed version    : 1.1.1k
```

tcp/0

```
Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
Reported version : 1.1.1f
Fixed version    : 1.1.1k
```

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

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1n
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1n
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1t
```

tcp/0

```
```

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  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

6.7

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1w
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  Fixed version    : 1.1.1w
```

135919 - OpenSSL 1.1.1d < 1.1.1g Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

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

- Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the signature_algorithms_cert TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f). (CVE-2020-1967)

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?d80da51b

https://www.cve.org/CVERecord?id=CVE-2020-1967

https://www.openssl.org/news/secadv/20200421.txt

Solution

Upgrade to OpenSSL version 1.1.1g 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

4.4

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-2020-1967
XREF	IAVA:2020-A-0186-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/04/23, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1g
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1g
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1g
```

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

6.7

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
overlay2/834484eb82b2041fa048b2a647874e9af27cb35ea471674c35c54e654f36dbdc/diff/lib/libcrypto.so.3
  Reported version : 3.0.8
  Fixed version    : 3.0.11
```

tcp/0

```


  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
overlay2/834484eb82b2041fa048b2a647874e9af27cb35ea471674c35c54e654f36dbdc/diff/lib/libcrypto.so.3
  Reported version : 3.0.8
  Fixed version    : 3.0.12
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

3.6

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

192219 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1)

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-6698-1 advisory.

- Vim before 9.0.2142 has a stack-based buffer overflow because did_set_langmap in map.c calls sprintf to write to the error buffer that is passed down to the option callback functions. (CVE-2024-22667)

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-6698-1

Solution

Update the affected packages.

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

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-2024-22667
XREF	USN:6698-1

Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

Plugin Output

tcp/0

```
  - Installed package : vim_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-common_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-common_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-runtime_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-runtime_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-tiny_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-tiny_2:8.2.3995-1ubuntu2.16

  - Installed package : xxd_2:8.2.3995-1ubuntu2.12
  - Fixed package     : xxd_2:8.2.3995-1ubuntu2.16
```

186711 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GNU Tar vulnerability (USN-6543-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6543-1 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-6543-1

Solution

Update the affected tar and / or tar-scripts 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

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-39804
XREF	USN:6543-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : tar_1.34+dfsg-1ubuntu0.1.22.04.1
  - Fixed package     : tar_1.34+dfsg-1ubuntu0.1.22.04.2
```

185930 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Intel Microcode vulnerability (USN-6485-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6485-1 advisory.

- Sequence of processor instructions leads to unexpected behavior for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege and/or information disclosure and/or denial of service via local access. (CVE-2023-23583)

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-6485-1

Solution

Update the affected intel-microcode 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

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-2023-23583
XREF	USN:6485-1

Plugin Information

Published: 2023/11/16, Modified: 2023/12/19

Plugin Output

tcp/0

```
  - Installed package : intel-microcode_3.20230808.0ubuntu0.22.04.1
  - Fixed package     : intel-microcode_3.20231114.0ubuntu0.22.04.1
```

183889 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Vim vulnerabilities (USN-6452-1)

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 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6452-1 advisory.

- Divide By Zero in vim/vim from 9.0.1367-1 to 9.0.1367-3 (CVE-2023-3896)

- Use After Free in GitHub repository vim/vim prior to 9.0.1840. (CVE-2023-4733)

- Integer Overflow or Wraparound in GitHub repository vim/vim prior to 9.0.1846. (CVE-2023-4734)

- Out-of-bounds Write in GitHub repository vim/vim prior to 9.0.1847. (CVE-2023-4735)

- Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1848. (CVE-2023-4738)

- Use After Free in GitHub repository vim/vim prior to 9.0.1857. (CVE-2023-4750)

- Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1331. (CVE-2023-4751)

- Use After Free in GitHub repository vim/vim prior to 9.0.1858. (CVE-2023-4752)

- Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1873. (CVE-2023-4781)

- Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1969. (CVE-2023-5344)

- NULL Pointer Dereference in GitHub repository vim/vim prior to 20d161ace307e28690229b68584f2d84556f8960.
(CVE-2023-5441)

- Use After Free in GitHub repository vim/vim prior to v9.0.2010. (CVE-2023-5535)

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-6452-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-3896
CVE	CVE-2023-4733
CVE	CVE-2023-4734
CVE	CVE-2023-4735
CVE	CVE-2023-4738
CVE	CVE-2023-4750
CVE	CVE-2023-4751
CVE	CVE-2023-4752
CVE	CVE-2023-4781
CVE	CVE-2023-5344
CVE	CVE-2023-5441
CVE	CVE-2023-5535
XREF	IAVB:2023-B-0066-S
XREF	IAVB:2023-B-0074-S
XREF	USN:6452-1
XREF	IAVB:2023-B-0084-S
XREF	IAVA:2023-A-0579-S

Plugin Information

Published: 2023/10/25, Modified: 2023/11/02

Plugin Output

tcp/0

```
  - Installed package : vim_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim_2:8.2.3995-1ubuntu2.13

  - Installed package : vim-common_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-common_2:8.2.3995-1ubuntu2.13

  - Installed package : vim-runtime_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-runtime_2:8.2.3995-1ubuntu2.13

  - Installed package : vim-tiny_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-tiny_2:8.2.3995-1ubuntu2.13

  - Installed package : xxd_2:8.2.3995-1ubuntu2.12
  - Fixed package     : xxd_2:8.2.3995-1ubuntu2.13
```

186991 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Vim vulnerabilities (USN-6557-1)

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 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6557-1 advisory.

- NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.4959. (CVE-2022-1725)

- Uncontrolled Recursion in GitHub repository vim/vim prior to 8.2.4975. (CVE-2022-1771)

- Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2. (CVE-2022-1886)

- Out-of-bounds Write in GitHub repository vim/vim prior to 8.2. (CVE-2022-1897, CVE-2022-2000)

- Use After Free in GitHub repository vim/vim prior to 8.2. (CVE-2022-2042)

- Vim is an improved version of the good old UNIX editor Vi. Heap-use-after-free in memory allocated in the function `ga_grow_inner` in in the file `src/alloc.c` at line 748, which is freed in the file `src/ex_docmd.c` in the function `do_cmdline` at line 1010 and then used again in `src/cmdhist.c` at line 759. When using the `:history` command, it's possible that the provided argument overflows the accepted value. Causing an Integer Overflow and potentially later an use-after-free. This vulnerability has been patched in version 9.0.2068. (CVE-2023-46246)

- Vim is an open source command line text editor. When closing a window, vim may try to access already freed window structure. Exploitation beyond crashing the application has not been shown to be viable. This issue has been addressed in commit `25aabc2b` which has been included in release version 9.0.2106. Users are advised to upgrade. There are no known workarounds for this vulnerability. (CVE-2023-48231)

- Vim is an open source command line text editor. A floating point exception may occur when calculating the line offset for overlong lines and smooth scrolling is enabled and the cpo-settings include the 'n' flag.

This may happen when a window border is present and when the wrapped line continues on the next physical line directly in the window border because the 'cpo' setting includes the 'n' flag. Only users with non- default settings are affected and the exception should only result in a crash. This issue has been addressed in commit `cb0b99f0` which has been included in release version 9.0.2107. Users are advised to upgrade. There are no known workarounds for this vulnerability. (CVE-2023-48232)

- Vim is an open source command line text editor. If the count after the :s command is larger than what fits into a (signed) long variable, abort with e_value_too_large. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `ac6378773` which has been included in release version 9.0.2108. Users are advised to upgrade. There are no known workarounds for this vulnerability. (CVE-2023-48233)

- Vim is an open source command line text editor. When getting the count for a normal mode z command, it may overflow for large counts given. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `58f9befca1` which has been included in release version 9.0.2109. Users are advised to upgrade. There are no known workarounds for this vulnerability. (CVE-2023-48234)

- Vim is an open source command line text editor. When parsing relative ex addresses one may unintentionally cause an overflow. Ironically this happens in the existing overflow check, because the line number becomes negative and LONG_MAX - lnum will cause the overflow. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `060623e` which has been included in release version 9.0.2110. Users are advised to upgrade. There are no known workarounds for this vulnerability. (CVE-2023-48235)

- Vim is an open source command line text editor. When using the z= command, the user may overflow the count with values larger than MAX_INT. Impact is low, user interaction is required and a crash may not even happen in all situations. This vulnerability has been addressed in commit `73b2d379` which has been included in release version 9.0.2111. Users are advised to upgrade. There are no known workarounds for this vulnerability. (CVE-2023-48236)

- Vim is an open source command line text editor. In affected versions when shifting lines in operator pending mode and using a very large value, it may be possible to overflow the size of integer. Impact is low, user interaction is required and a crash may not even happen in all situations. This issue has been addressed in commit `6bf131888` which has been included in version 9.0.2112. Users are advised to upgrade.

There are no known workarounds for this vulnerability. (CVE-2023-48237)

- Vim is a UNIX editor that, prior to version 9.0.2121, has a heap-use-after-free vulnerability. When executing a `:s` command for the very first time and using a sub-replace-special atom inside the substitution part, it is possible that the recursive `:s` call causes free-ing of memory which may later then be accessed by the initial `:s` command. The user must intentionally execute the payload and the whole process is a bit tricky to do since it seems to work only reliably for the very first :s command. It may also cause a crash of Vim. Version 9.0.2121 contains a fix for this issue. (CVE-2023-48706)

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-6557-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

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-2022-1725
CVE	CVE-2022-1771
CVE	CVE-2022-1886
CVE	CVE-2022-1897
CVE	CVE-2022-2000
CVE	CVE-2022-2042
CVE	CVE-2023-46246
CVE	CVE-2023-48231
CVE	CVE-2023-48232
CVE	CVE-2023-48233
CVE	CVE-2023-48234
CVE	CVE-2023-48235
CVE	CVE-2023-48236
CVE	CVE-2023-48237
CVE	CVE-2023-48706
XREF	IAVA:2023-A-0598-S
XREF	IAVA:2023-A-0650
XREF	IAVB:2022-B-0049-S
XREF	USN:6557-1

Plugin Information

Published: 2023/12/15, Modified: 2023/12/15

Plugin Output

tcp/0

```
  - Installed package : vim_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim_2:8.2.3995-1ubuntu2.15

  - Installed package : vim-common_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-common_2:8.2.3995-1ubuntu2.15
  - Installed package : vim-runtime_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-runtime_2:8.2.3995-1ubuntu2.15

  - Installed package : vim-tiny_2:8.2.3995-1ubuntu2.12
  - Fixed package     : vim-tiny_2:8.2.3995-1ubuntu2.15

  - Installed package : xxd_2:8.2.3995-1ubuntu2.12
  - Fixed package     : xxd_2:8.2.3995-1ubuntu2.15
```

185342 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : urllib3 vulnerabilities (USN-6473-1)

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 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6473-1 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-6473-1

Solution

Update the affected python-urllib3 and / or python3-urllib3 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

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:6473-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : python3-urllib3_1.26.5-1~exp1
  - Fixed package     : python3-urllib3_1.26.5-1~exp1ubuntu0.1
```

186676 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : GNU C Library vulnerabilities (USN-6541-1)

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-6541-1 advisory.

- A flaw was found in glibc. In an extremely rare situation, the getaddrinfo function may access memory that has been freed, resulting in an application crash. This issue is only exploitable when a NSS module implements only the _nss_*_gethostbyname2_r and _nss_*_getcanonname_r hooks without implementing the

_nss_*_gethostbyname3_r hook. The resolved name should return a large number of IPv6 and IPv4, and the call to the getaddrinfo function should have the AF_INET6 address family with AI_CANONNAME, AI_ALL and AI_V4MAPPED as flags. (CVE-2023-4806)

- A flaw was found in glibc. In an uncommon situation, the gaih_inet function may use memory that has been freed, resulting in an application crash. This issue is only exploitable when the getaddrinfo function is called and the hosts database in /etc/nsswitch.conf is configured with SUCCESS=continue or SUCCESS=merge.

(CVE-2023-4813)

- A flaw was found in the GNU C Library. A recent fix for CVE-2023-4806 introduced the potential for a memory leak, which may result in an application crash. (CVE-2023-5156)

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-6541-1

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

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-2023-4806
CVE	CVE-2023-4813
CVE	CVE-2023-5156
XREF	USN:6541-1

Plugin Information

Published: 2023/12/07, Modified: 2023/12/07

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.4
  - Fixed package     : libc-bin_2.35-0ubuntu3.5

  - Installed package : libc6_2.35-0ubuntu3.4
  - Fixed package     : libc6_2.35-0ubuntu3.5

  - Installed package : locales_2.35-0ubuntu3.4
  - Fixed package     : locales_2.35-0ubuntu3.5
```

198244 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6804-1 advisory.

It was discovered that GNU C Library nscd daemon contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33599)

It was discovered that GNU C Library nscd daemon did not properly check the cache content, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33600)

It was discovered that GNU C Library nscd daemon did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33601)

It was discovered that GNU C Library nscd daemon did not properly handle memory allocation, which could lead to memory corruption. A local attacker could use this to cause a denial of service (system crash).

(CVE-2024-33602)

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-6804-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-33599
CVE	CVE-2024-33600
CVE	CVE-2024-33601
CVE	CVE-2024-33602
XREF	USN:6804-1

Plugin Information

Published: 2024/05/31, Modified: 2024/05/31

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.4
  - Fixed package     : libc-bin_2.35-0ubuntu3.8

  - Installed package : libc6_2.35-0ubuntu3.4
  - Fixed package     : libc6_2.35-0ubuntu3.8

  - Installed package : locales_2.35-0ubuntu3.4
  - Fixed package     : locales_2.35-0ubuntu3.8
```

198069 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Intel Microcode vulnerabilities (USN-6797-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6797-1 advisory.

It was discovered that some 3rd and 4th Generation Intel Xeon Processors did not properly restrict access to certain hardware features when using Intel SGX or Intel TDX. This may allow a privileged local user to potentially further escalate their privileges on the system. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-22655)

It was discovered that some Intel Atom Processors did not properly clear register state when performing various operations. A local attacker could use this to obtain sensitive information via a transient execution attack. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-28746)

It was discovered that some Intel Processors did not properly clear the state of various hardware structures when switching execution contexts. A local attacker could use this to access privileged information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-38575)

It was discovered that some Intel Processors did not properly enforce bus lock regulator protections. A remote attacker could use this to cause a denial of service. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-39368)

It was discovered that some Intel Xeon D Processors did not properly calculate the SGX base key when using Intel SGX. A privileged local attacker could use this to obtain sensitive information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS.

(CVE-2023-43490)

It was discovered that some Intel Processors did not properly protect against concurrent accesses. A local attacker could use this to obtain sensitive information. (CVE-2023-45733)

It was discovered that some Intel Processors TDX module software did not properly validate input. A privileged local attacker could use this information to potentially further escalate their privileges on the system. (CVE-2023-45745, CVE-2023-47855)

It was discovered that some Intel Core Ultra processors did not properly handle particular instruction sequences. A local attacker could use this issue to cause a denial of service.

(CVE-2023-46103)

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-6797-1

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22655
CVE	CVE-2023-28746
CVE	CVE-2023-38575
CVE	CVE-2023-39368
CVE	CVE-2023-43490
CVE	CVE-2023-45733
CVE	CVE-2023-45745
CVE	CVE-2023-46103
CVE	CVE-2023-47855
XREF	USN:6797-1

Plugin Information

Published: 2024/05/29, Modified: 2024/05/29

Plugin Output

tcp/0

```
  - Installed package : intel-microcode_3.20230808.0ubuntu0.22.04.1
  - Fixed package     : intel-microcode_3.20240514.0ubuntu0.22.04.1
```

193905 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1)

Synopsis

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

Description

The remote Ubuntu 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-6754-1 advisory.

- Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both. (CVE-2019-9511)

- Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service.

The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU. (CVE-2019-9513)

- The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. (CVE-2023-44487)

- nghttp2 is an implementation of the Hypertext Transfer Protocol version 2 in C. The nghttp2 library prior to version 1.61.0 keeps reading the unbounded number of HTTP/2 CONTINUATION frames even after a stream is reset to keep HPACK context in sync. This causes excessive CPU usage to decode HPACK stream. nghttp2 v1.61.0 mitigates this vulnerability by limiting the number of CONTINUATION frames it accepts per stream.

There is no workaround for this vulnerability. (CVE-2024-28182)

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-6754-1

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

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

VPR Score

6.1

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

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

References

CVE	CVE-2019-9511
CVE	CVE-2019-9513
CVE	CVE-2023-44487
CVE	CVE-2024-28182
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	USN:6754-1
XREF	CEA-ID:CEA-2024-0004
XREF	CEA-ID:CEA-2019-0643

Plugin Information

Published: 2024/04/25, Modified: 2024/04/26

Plugin Output

tcp/0

```
  - Installed package : libnghttp2-14_1.43.0-1build3
  - Fixed package     : libnghttp2-14_1.43.0-1ubuntu0.2
```

175916 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.04 : libwebp vulnerability (USN-6078-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6078-1 advisory.

- A double-free in libwebp could have led to memory corruption and a potentially exploitable crash.

(CVE-2023-1999)

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-6078-1

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

3.6

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-2023-1999
XREF	USN:6078-1

Plugin Information

Published: 2023/05/17, Modified: 2023/10/16

Plugin Output

tcp/0

```
  - Installed package : libwebp7_1.2.2-2
  - Fixed package     : libwebp7_1.2.2-2ubuntu0.22.04.1
```

191499 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : python-cryptography vulnerabilities (USN-6673-1)

Synopsis

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

Description

The remote Ubuntu 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-6673-1 advisory.

- A flaw was found in the python-cryptography package. This issue may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data. (CVE-2023-50782)

- cryptography is a package designed to expose cryptographic primitives and recipes to Python developers.

Starting in version 38.0.0 and prior to version 42.0.4, if `pkcs12.serialize_key_and_certificates` is called with both a certificate whose public key did not match the provided private key and an `encryption_algorithm` with `hmac_hash` set (via `PrivateFormat.PKCS12.encryption_builder().hmac_hash(...)`, then a NULL pointer dereference would occur, crashing the Python process. This has been resolved in version 42.0.4, the first version in which a `ValueError` is properly raised. (CVE-2024-26130)

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-6673-1

Solution

Update the affected python-cryptography and / or python3-cryptography 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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

3.6

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)

References

CVE	CVE-2023-50782
CVE	CVE-2024-26130
XREF	USN:6673-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : python3-cryptography_3.4.8-1ubuntu2
  - Fixed package     : python3-cryptography_3.4.8-1ubuntu2.2
```

168337 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerability (USN-5743-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 host has packages installed that are affected by a vulnerability as referenced in the USN-5743-2 advisory.

- A vulnerability was found in LibTIFF. It has been classified as critical. This affects the function TIFFReadRGBATileExt of the file libtiff/tif_getimage.c. The manipulation leads to integer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.

The name of the patch is 227500897dfb07fb7d27f7aa570050e62617e3be. It is recommended to apply a patch to fix this issue. The identifier VDB-213549 was assigned to this vulnerability. (CVE-2022-3970)

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-5743-2

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/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

6.7

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)

References

CVE	CVE-2022-3970
XREF	USN:5743-2

Plugin Information

Published: 2022/12/02, Modified: 2023/11/01

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.3
```

172048 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : c-ares vulnerability (USN-5907-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5907-1 advisory.

- buffer overflow in config_sortlist() due to missing string length check [fedora-all] (CVE-2022-4904)

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-5907-1

Solution

Update the affected libc-ares-dev and / or libc-ares2 packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-4904
XREF	USN:5907-1

Plugin Information

Published: 2023/03/02, Modified: 2023/10/16

Plugin Output

tcp/0

```
  - Installed package : libc-ares2_1.18.1-1build1
  - Fixed package     : libc-ares2_1.18.1-1ubuntu0.22.04.1
```

189294 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GnuTLS vulnerabilities (USN-6593-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6593-1 advisory.

- A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981. (CVE-2024-0553)

- A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure.

This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack.

(CVE-2024-0567)

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-6593-1

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:H/I:N/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

4.4

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

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

References

CVE	CVE-2024-0553
CVE	CVE-2024-0567
XREF	USN:6593-1

Plugin Information

Published: 2024/01/22, Modified: 2024/01/25

Plugin Output

tcp/0

```

  - Installed package : libgnutls30_3.7.3-4ubuntu1.2
  - Fixed package     : libgnutls30_3.7.3-4ubuntu1.4

```

184088 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Open VM Tools vulnerabilities (USN-6463-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6463-1 advisory.

- VMware Tools contains a SAML token signature bypass vulnerability. A malicious actor that has been granted Guest Operation Privileges https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere- security/GUID-6A952214-0E5E-4CCF-9D2A-90948FF643EC.html in a target virtual machine may be able to elevate their privileges if that target virtual machine has been assigned a more privileged Guest Alias https://vdc-download.vmware.com/vmwb-repository/dcr-public/d1902b0e-d479-46bf-8ac9-cee0e31e8ec0/07ce8dbd-db48-4261-9b8f-c6d3ad8ba472/vim.vm.guest.AliasManager.html . (CVE-2023-34058)

- open-vm-tools contains a file descriptor hijack vulnerability in the vmware-user-suid-wrapper. A malicious actor with non-root privileges may be able to hijack the /dev/uinput file descriptor allowing them to simulate user inputs. (CVE-2023-34059)

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-6463-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-34058
CVE	CVE-2023-34059
XREF	USN:6463-1

Plugin Information

Published: 2023/10/31, Modified: 2023/10/31

Plugin Output

tcp/0

```
  - Installed package : open-vm-tools_2:12.1.5-3~ubuntu0.22.04.3
  - Fixed package     : open-vm-tools_2:12.1.5-3~ubuntu0.22.04.4
```

187627 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : OpenSSH vulnerabilities (USN-6565-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6565-1 advisory.

- sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
(CVE-2021-41617)

- In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys. (CVE-2023-51384)

- In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.
(CVE-2023-51385)

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-6565-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-41617
CVE	CVE-2023-51384
CVE	CVE-2023-51385
XREF	IAVA:2021-A-0474-S
XREF	IAVA:2023-A-0701
XREF	USN:6565-1

Plugin Information

Published: 2024/01/03, Modified: 2024/01/03

Plugin Output

tcp/0

```
  - Installed package : openssh-client_1:8.9p1-3ubuntu0.3
  - Fixed package     : openssh-client_1:8.9p1-3ubuntu0.6

  - Installed package : openssh-server_1:8.9p1-3ubuntu0.3
  - Fixed package     : openssh-server_1:8.9p1-3ubuntu0.6

  - Installed package : openssh-sftp-server_1:8.9p1-3ubuntu0.3
  - Fixed package     : openssh-sftp-server_1:8.9p1-3ubuntu0.6
```

187626 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : SQLite vulnerabilities (USN-6566-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6566-1 advisory.

- SQLite through 3.40.0, when relying on --safe for execution of an untrusted CLI script, does not properly implement the azProhibitedFunctions protection mechanism, and instead allows UDF functions such as WRITEFILE. (CVE-2022-46908)

- A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999. (CVE-2023-7104)

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-6566-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.3

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

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

STIG Severity

I

References

CVE	CVE-2022-46908
CVE	CVE-2023-7104
XREF	IAVA:2023-A-0006-S
XREF	USN:6566-1
XREF	IAVA:2024-A-0003

Plugin Information

Published: 2024/01/03, Modified: 2024/01/09

Plugin Output

tcp/0

```
  - Installed package : libsqlite3-0_3.37.2-2ubuntu0.1
  - Fixed package     : libsqlite3-0_3.37.2-2ubuntu0.3
```

186192 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : nghttp2 vulnerability (USN-6505-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6505-1 advisory.

- The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. (CVE-2023-44487)

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-6505-1

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

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

VPR Score

6.1

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

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

References

CVE	CVE-2023-44487
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	USN:6505-1
XREF	CEA-ID:CEA-2024-0004

Plugin Information

Published: 2023/11/22, Modified: 2024/02/09

Plugin Output

tcp/0

```
  - Installed package : libnghttp2-14_1.43.0-1build3
  - Fixed package     : libnghttp2-14_1.43.0-1ubuntu0.1
```

181426 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libwebp vulnerability (USN-6369-1)

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-6369-1 advisory.

- Heap buffer overflow in WebP in Google Chrome prior to 116.0.5845.187 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical) (CVE-2023-4863)

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-6369-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.4 (CVSS:3.0/E:H/RL:O/RC:C)

VPR Score

9.8

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

8.7 (CVSS2#E:H/RL:OF/RC:C)

References

CVE	CVE-2023-4863
XREF	CISA-KNOWN-EXPLOITED:2023/10/04
XREF	USN:6369-1

Plugin Information

Published: 2023/09/14, Modified: 2023/10/20

Plugin Output

tcp/0

```
  - Installed package : libwebp7_1.2.2-2
  - Fixed package     : libwebp7_1.2.2-2ubuntu0.22.04.2
```

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

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 : libglib2.0-0_2.72.4-0ubuntu2.2
  - Fixed package     : libglib2.0-0_2.72.4-0ubuntu2.3

  - Installed package : libglib2.0-bin_2.72.4-0ubuntu2.2
  - Fixed package     : libglib2.0-bin_2.72.4-0ubuntu2.3

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

192621 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1)

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-6718-1 advisory.

- When a protocol selection parameter option disables all protocols without adding any then the default set of protocols would remain in the allowed set due to an error in the logic for removing protocols. The below command would perform a request to curl.se with a plaintext protocol which has been explicitly disabled. curl --proto -all,-http http://curl.se The flaw is only present if the set of selected protocols disables the entire set of available protocols, in itself a command with no practical use and therefore unlikely to be encountered in real situations. The curl security team has thus assessed this to be low severity bug. (CVE-2024-2004)

- 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.

(CVE-2024-2398)

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-6718-1

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

4.4

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-2024-2004
CVE	CVE-2024-2398
XREF	USN:6718-1
XREF	IAVA:2024-A-0185

Plugin Information

Published: 2024/03/27, Modified: 2024/03/29

Plugin Output

tcp/0

```
  - Installed package : curl_7.81.0-1ubuntu1.14
  - Fixed package     : curl_7.81.0-1ubuntu1.16

  - Installed package : libcurl3-gnutls_7.81.0-1ubuntu1.14
  - Fixed package     : libcurl3-gnutls_7.81.0-1ubuntu1.16

  - Installed package : libcurl4_7.81.0-1ubuntu1.14
  - Fixed package     : libcurl4_7.81.0-1ubuntu1.16
```

191103 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : libuv vulnerability (USN-6666-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6666-1 advisory.

- libuv is a multi-platform support library with a focus on asynchronous I/O. The `uv_getaddrinfo` function in `src/unix/getaddrinfo.c` (and its windows counterpart `src/win/getaddrinfo.c`), truncates hostnames to 256 characters before calling `getaddrinfo`. This behavior can be exploited to create addresses like `0x00007f000001`, which are considered valid by `getaddrinfo` and could allow an attacker to craft payloads that resolve to unintended IP addresses, bypassing developer checks. The vulnerability arises due to how the `hostname_ascii` variable (with a length of 256 bytes) is handled in `uv_getaddrinfo` and subsequently in `uv__idna_toascii`. When the hostname exceeds 256 characters, it gets truncated without a terminating null byte. As a result attackers may be able to access internal APIs or for websites (similar to MySpace) that allows users to have `username.example.com` pages. Internal services that crawl or cache these user pages can be exposed to SSRF attacks if a malicious user chooses a long vulnerable username.

This issue has been addressed in release version 1.48.0. Users are advised to upgrade. There are no known workarounds for this vulnerability. (CVE-2024-24806)

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-6666-1

Solution

Update the affected libuv1 and / or libuv1-dev packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.9

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

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

References

CVE	CVE-2024-24806
XREF	USN:6666-1

Plugin Information

Published: 2024/02/28, Modified: 2024/03/11

Plugin Output

tcp/0

```
  - Installed package : libuv1_1.43.0-1
  - Fixed package     : libuv1_1.43.0-1ubuntu0.1
```

191019 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : libxml2 vulnerability (USN-6658-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6658-1 advisory.

- An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free. (CVE-2024-25062)

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-6658-1

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

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

VPR Score

4.4

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

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

STIG Severity

II

References

CVE	CVE-2024-25062
XREF	IAVA:2024-A-0067
XREF	USN:6658-1

Plugin Information

Published: 2024/02/26, Modified: 2024/03/11

Plugin Output

tcp/0

```
  - Installed package : libxml2_2.9.13+dfsg-1ubuntu0.3
  - Fixed package     : libxml2_2.9.13+dfsg-1ubuntu0.4
```

192629 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-1 advisory.

- wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover. (CVE-2024-28085)

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-6719-1

Solution

Update the affected packages.

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

7.9

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

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

References

CVE	CVE-2024-28085
XREF	USN:6719-1

Plugin Information

Published: 2024/03/27, Modified: 2024/03/29

Plugin Output

tcp/0

```

  - Installed package : bsdextrautils_2.37.2-4ubuntu3
  - Fixed package     : bsdextrautils_2.37.2-4ubuntu3.3

  - Installed package : bsdutils_1:2.37.2-4ubuntu3
  - Fixed package     : bsdutils_1:2.37.2-4ubuntu3.3

  - Installed package : eject_2.37.2-4ubuntu3
  - Fixed package     : eject_2.37.2-4ubuntu3.3

  - Installed package : fdisk_2.37.2-4ubuntu3
  - Fixed package     : fdisk_2.37.2-4ubuntu3.3

  - Installed package : libblkid1_2.37.2-4ubuntu3
  - Fixed package     : libblkid1_2.37.2-4ubuntu3.3

  - Installed package : libfdisk1_2.37.2-4ubuntu3
  - Fixed package     : libfdisk1_2.37.2-4ubuntu3.3

  - Installed package : libmount1_2.37.2-4ubuntu3
  - Fixed package     : libmount1_2.37.2-4ubuntu3.3

  - Installed package : libsmartcols1_2.37.2-4ubuntu3
  - Fixed package     : libsmartcols1_2.37.2-4ubuntu3.3

  - Installed package : libuuid1_2.37.2-4ubuntu3
  - Fixed package     : libuuid1_2.37.2-4ubuntu3.3

  - Installed package : mount_2.37.2-4ubuntu3
  - Fixed package     : mount_2.37.2-4ubuntu3.3

  - Installed package : util-linux_2.37.2-4ubuntu3
  - Fixed package     : util-linux_2.37.2-4ubuntu3.3

  - Installed package : uuid-runtime_2.37.2-4ubuntu3
  - Fixed package     : uuid-runtime_2.37.2-4ubuntu3.3
```

193159 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-2 advisory.

- wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover. (CVE-2024-28085)

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-6719-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28085
XREF	USN:6719-2

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : bsdextrautils_2.37.2-4ubuntu3
  - Fixed package     : bsdextrautils_2.37.2-4ubuntu3.4

  - Installed package : bsdutils_1:2.37.2-4ubuntu3
  - Fixed package     : bsdutils_1:2.37.2-4ubuntu3.4

  - Installed package : eject_2.37.2-4ubuntu3
  - Fixed package     : eject_2.37.2-4ubuntu3.4

  - Installed package : fdisk_2.37.2-4ubuntu3
  - Fixed package     : fdisk_2.37.2-4ubuntu3.4

  - Installed package : libblkid1_2.37.2-4ubuntu3
  - Fixed package     : libblkid1_2.37.2-4ubuntu3.4

  - Installed package : libfdisk1_2.37.2-4ubuntu3
  - Fixed package     : libfdisk1_2.37.2-4ubuntu3.4

  - Installed package : libmount1_2.37.2-4ubuntu3
  - Fixed package     : libmount1_2.37.2-4ubuntu3.4

  - Installed package : libsmartcols1_2.37.2-4ubuntu3
  - Fixed package     : libsmartcols1_2.37.2-4ubuntu3.4

  - Installed package : libuuid1_2.37.2-4ubuntu3
  - Fixed package     : libuuid1_2.37.2-4ubuntu3.4

  - Installed package : mount_2.37.2-4ubuntu3
  - Fixed package     : mount_2.37.2-4ubuntu3.4

  - Installed package : util-linux_2.37.2-4ubuntu3
  - Fixed package     : util-linux_2.37.2-4ubuntu3.4

  - Installed package : uuid-runtime_2.37.2-4ubuntu3
  - Fixed package     : uuid-runtime_2.37.2-4ubuntu3.4
```

186720 - Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6544-1)

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-6544-1 advisory.

- An issue was discovered in binutils libbfd.c 2.36 relating to the auxiliary symbol data allows attackers to read or write to system memory or cause a denial of service. (CVE-2020-19726)

- Heap-based Buffer Overflow in function bfd_getl32 in Binutils objdump 3.37. (CVE-2021-46174)

- An issue was discovered in Binutils readelf 2.38.50, reachable assertion failure in function display_debug_names allows attackers to cause a denial of service. (CVE-2022-35205)

- In GNU Binutils before 2.40, there is a heap-buffer-overflow in the error function bfd_getl32 when called from the strip_main function in strip-new via a crafted file. (CVE-2022-38533)

- An illegal memory access flaw was found in the binutils package. Parsing an ELF file containing corrupt symbol version information may result in a denial of service. This issue is the result of an incomplete fix for CVE-2020-16599. (CVE-2022-4285)

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-6544-1

Solution

Update the affected packages.

Risk Factor

Critical

CVSS v3.0 Base Score

8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/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

6.7

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)

References

CVE	CVE-2020-19726
CVE	CVE-2021-46174
CVE	CVE-2022-4285
CVE	CVE-2022-35205
CVE	CVE-2022-38533
XREF	USN:6544-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : binutils_2.38-4ubuntu2.3
  - Fixed package     : binutils_2.38-4ubuntu2.4

  - Installed package : binutils-common_2.38-4ubuntu2.3
  - Fixed package     : binutils-common_2.38-4ubuntu2.4

  - Installed package : binutils-x86-64-linux-gnu_2.38-4ubuntu2.3
  - Fixed package     : binutils-x86-64-linux-gnu_2.38-4ubuntu2.4

  - Installed package : libbinutils_2.38-4ubuntu2.3
  - Fixed package     : libbinutils_2.38-4ubuntu2.4

  - Installed package : libctf-nobfd0_2.38-4ubuntu2.3
  - Fixed package     : libctf-nobfd0_2.38-4ubuntu2.4

  - Installed package : libctf0_2.38-4ubuntu2.3
  - Fixed package     : libctf0_2.38-4ubuntu2.4
```

188049 - Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6581-1)

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-6581-1 advisory.

- Heap buffer overflow vulnerability in binutils readelf before 2.40 via function find_section_in_set in file readelf.c. (CVE-2022-44840)

- Heap buffer overflow vulnerability in binutils readelf before 2.40 via function display_debug_section in file readelf.c. (CVE-2022-45703)

- An issue was discovered function stab_demangle_v3_arg in stabs.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks. (CVE-2022-47007)

- An issue was discovered function make_tempdir, and make_tempname in bucomm.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks. (CVE-2022-47008)

- An issue was discovered function pr_function_type in prdbg.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks. (CVE-2022-47010)

- An issue was discovered function parse_stab_struct_fields in stabs.c in Binutils 2.34 thru 2.38, allows attackers to cause a denial of service due to memory leaks. (CVE-2022-47011)

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-6581-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-44840
CVE	CVE-2022-45703
CVE	CVE-2022-47007
CVE	CVE-2022-47008
CVE	CVE-2022-47010
CVE	CVE-2022-47011
XREF	USN:6581-1

Plugin Information

Published: 2024/01/15, Modified: 2024/01/15

Plugin Output

tcp/0

```
  - Installed package : binutils_2.38-4ubuntu2.3
  - Fixed package     : binutils_2.38-4ubuntu2.5

  - Installed package : binutils-common_2.38-4ubuntu2.3
  - Fixed package     : binutils-common_2.38-4ubuntu2.5

  - Installed package : binutils-x86-64-linux-gnu_2.38-4ubuntu2.3
  - Fixed package     : binutils-x86-64-linux-gnu_2.38-4ubuntu2.5

  - Installed package : libbinutils_2.38-4ubuntu2.3
  - Fixed package     : libbinutils_2.38-4ubuntu2.5

  - Installed package : libctf-nobfd0_2.38-4ubuntu2.3
  - Fixed package     : libctf-nobfd0_2.38-4ubuntu2.5

  - Installed package : libctf0_2.38-4ubuntu2.3
  - Fixed package     : libctf0_2.38-4ubuntu2.5
```

191003 - Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils vulnerabilities (USN-6655-1)

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-6655-1 advisory.

- An issue was discovered Binutils objdump before 2.39.3 allows attackers to cause a denial of service or other unspecified impacts via function bfd_mach_o_get_synthetic_symtab in match-o.c. (CVE-2022-47695)

- GNU Binutils before 2.40 was discovered to contain an excessive memory consumption vulnerability via the function load_separate_debug_files at dwarf2.c. The attacker could supply a crafted ELF file and cause a DNS attack. (CVE-2022-48063)

- GNU Binutils before 2.40 was discovered to contain a memory leak vulnerability var the function find_abstract_instance in dwarf2.c. (CVE-2022-48065)

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-6655-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-47695
CVE	CVE-2022-48063
CVE	CVE-2022-48065
XREF	USN:6655-1

Plugin Information

Published: 2024/02/26, Modified: 2024/03/11

Plugin Output

tcp/0

```
  - Installed package : binutils_2.38-4ubuntu2.3
  - Fixed package     : binutils_2.38-4ubuntu2.6

  - Installed package : binutils-common_2.38-4ubuntu2.3
  - Fixed package     : binutils-common_2.38-4ubuntu2.6

  - Installed package : binutils-x86-64-linux-gnu_2.38-4ubuntu2.3
  - Fixed package     : binutils-x86-64-linux-gnu_2.38-4ubuntu2.6

  - Installed package : libbinutils_2.38-4ubuntu2.3
  - Fixed package     : libbinutils_2.38-4ubuntu2.6

  - Installed package : libctf-nobfd0_2.38-4ubuntu2.3
  - Fixed package     : libctf-nobfd0_2.38-4ubuntu2.6

  - Installed package : libctf0_2.38-4ubuntu2.3
  - Fixed package     : libctf0_2.38-4ubuntu2.6
```

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

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

8.4

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

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

6.7

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

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

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

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

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

6.7

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.
```

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

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-2.5-0_2.5.15+dfsg-0ubuntu0.22.04.1
  - Fixed package     : libldap-2.5-0_2.5.16+dfsg-0ubuntu0.22.04.2

  - Installed package : libldap-common_2.5.15+dfsg-0ubuntu0.22.04.1
  - Fixed package     : libldap-common_2.5.16+dfsg-0ubuntu0.22.04.2
```

183790 - Ubuntu 22.04 LTS / 23.04 / 23.10 : OpenSSL vulnerabilities (USN-6450-1)

Synopsis

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

Description

The remote Ubuntu 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6450-1 advisory.

- 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)

- 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: 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)

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-6450-1

Solution

Update the affected libssl-dev, libssl3 and / or openssl 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: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

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-2023-2975
CVE	CVE-2023-3446
CVE	CVE-2023-3817
CVE	CVE-2023-5363

XREF	IAVA:2023-A-0398-S
XREF	USN:6450-1
XREF	IAVA:2023-A-0582-S

Plugin Information

Published: 2023/10/24, Modified: 2024/03/08

Plugin Output

tcp/0

```
  - Installed package : libssl3_3.0.2-0ubuntu1.10
  - Fixed package     : libssl3_3.0.2-0ubuntu1.12

  - Installed package : openssl_3.0.2-0ubuntu1.10
  - Fixed package     : openssl_3.0.2-0ubuntu1.12
```

200099 - Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : libarchive vulnerability (USN-6805-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6805-1 advisory.

It was discovered that libarchive incorrectly handled certain RAR archive files. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

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-6805-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-26256
XREF	USN:6805-1

Plugin Information

Published: 2024/06/04, Modified: 2024/06/04

Plugin Output

tcp/0

```
  - Installed package : libarchive13_3.6.0-1ubuntu1
  - Fixed package     : libarchive13_3.6.0-1ubuntu1.1
```

190450 - Ubuntu 22.04 LTS / 23.10 : Bind vulnerabilities (USN-6633-1)

Synopsis

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

Description

The remote Ubuntu 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6633-1 advisory.

- The DNS message parsing code in `named` includes a section whose computational complexity is overly high.

It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected `named` instance by exploiting this flaw. This issue affects both authoritative servers and recursive resolvers. This issue affects BIND 9 versions 9.0.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1. (CVE-2023-4408)

- A flaw in query-handling code can cause `named` to exit prematurely with an assertion failure when: - `nxdomain-redirect <domain>;` is configured, and - the resolver receives a PTR query for an RFC 1918 address that would normally result in an authoritative NXDOMAIN response. This issue affects BIND 9 versions 9.12.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1. (CVE-2023-5517)

- A bad interaction between DNS64 and serve-stale may cause `named` to crash with an assertion failure during recursive resolution, when both of these features are enabled. This issue affects BIND 9 versions 9.16.12 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.16.12-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1. (CVE-2023-5679)

- MITRE: CVE-2023-50387 DNSSEC verification complexity can be exploited to exhaust CPU resources and stall DNS resolvers (CVE-2023-50387)

- The processing of responses coming from DNSSEC-signed zones using NSEC3 can cause CPU exhaustion on a DNSSEC-validating resolver.By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service. (CVE-2023-50868)

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-6633-1

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

5.1

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-2023-4408
CVE	CVE-2023-5517
CVE	CVE-2023-5679
CVE	CVE-2023-50387
CVE	CVE-2023-50868
XREF	USN:6633-1
XREF	IAVA:2024-A-0103

Plugin Information

Published: 2024/02/13, Modified: 2024/02/16

Plugin Output

tcp/0

```
  - Installed package : bind9-dnsutils_1:9.18.12-0ubuntu0.22.04.3
  - Fixed package     : bind9-dnsutils_1:9.18.18-0ubuntu0.22.04.2

  - Installed package : bind9-host_1:9.18.12-0ubuntu0.22.04.3
  - Fixed package     : bind9-host_1:9.18.18-0ubuntu0.22.04.2

  - Installed package : bind9-libs_1:9.18.12-0ubuntu0.22.04.3
  - Fixed package     : bind9-libs_1:9.18.18-0ubuntu0.22.04.2
```

192118 - Ubuntu 22.04 LTS / 23.10 : Expat vulnerabilities (USN-6694-1)

Synopsis

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

Description

The remote Ubuntu 22.04 LTS / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6694-1 advisory.

- libexpat through 2.5.0 allows a denial of service (resource consumption) because many full reparsings are required in the case of a large token for which multiple buffer fills are needed. (CVE-2023-52425)

- libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of external parsers (created via XML_ExternalEntityParserCreate). (CVE-2024-28757)

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-6694-1

Solution

Update the affected expat, libexpat1 and / or libexpat1-dev 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

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

VPR Score

4.4

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

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

STIG Severity

I

References

CVE	CVE-2023-52425
CVE	CVE-2024-28757
XREF	USN:6694-1
XREF	IAVA:2024-A-0134-S
XREF	IAVA:2024-A-0192

Plugin Information

Published: 2024/03/14, Modified: 2024/04/05

Plugin Output

tcp/0

```
  - Installed package : libexpat1_2.4.7-1ubuntu0.2
  - Fixed package     : libexpat1_2.4.7-1ubuntu0.3
```

192198 - Ubuntu 22.04 LTS : Bash vulnerability (USN-6697-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6697-1 advisory.

- A flaw was found in the bash package, where a heap-buffer overflow can occur in valid parameter_transform.

This issue may lead to memory problems. (CVE-2022-3715)

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-6697-1

Solution

Update the affected bash, bash-builtins and / or bash-static packages.

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

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-2022-3715
XREF	USN:6697-1

Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

Plugin Output

tcp/0

```
  - Installed package : bash_5.1-6ubuntu1
  - Fixed package     : bash_5.1-6ubuntu1.1
```

191065 - Ubuntu 22.04 LTS : LibTIFF vulnerabilities (USN-6644-2)

Synopsis

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

Description

The remote Ubuntu 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6644-2 advisory.

- A segment fault (SEGV) flaw was found in libtiff that could be triggered by passing a crafted tiff file to the TIFFReadRGBATileExt() API. This flaw allows a remote attacker to cause a heap-buffer overflow, leading to a denial of service. (CVE-2023-52356)

- An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash. (CVE-2023-6228)

- An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may allow a remote attacker to cause a denial of service via a craft input with size smaller than 379 KB.

(CVE-2023-6277)

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-6644-2

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

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

VPR Score

4.4

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

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

References

CVE	CVE-2023-52356
CVE	CVE-2023-6228
CVE	CVE-2023-6277
XREF	USN:6644-2

Plugin Information

Published: 2024/02/27, Modified: 2024/03/11

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.8
```

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

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
```

144047 - OpenSSL 1.1.1 < 1.1.1i Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

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

- The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified.

OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue.

Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971)

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?1f13c66b

https://www.cve.org/CVERecord?id=CVE-2020-1971

https://www.openssl.org/news/secadv/20201208.txt

Solution

Upgrade to OpenSSL version 1.1.1i 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

6.1

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-2020-1971
XREF	IAVA:2020-A-0566-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/10, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1i
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
```

```
    Fixed version    : 1.1.1i
```

tcp/0

```


    Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
    Reported version : 1.1.1f
    Fixed version    : 1.1.1i
```

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

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             : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1q
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  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

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1u
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1u
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  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

2.9

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1v
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1v
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version     : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  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

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              : /snap/core20/1974/usr/bin/openssl
  Reported version : 1.1.1f
  Fixed version     : 1.1.1x
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  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

5.9

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              : /snap/core20/1974/usr/bin/openssl
Reported version : 1.1.1f
Fixed version     : 1.1.1y
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libssl.so.1.1
  Reported version : 1.1.1f
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/45e15af69a8befb6e309c2bf66ff3ea73434b74b3bea1550122a9702144b07b3/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/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/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/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/
overlay2/9258edb461881aca814601808f0efd205f59f9bf03b87ddf9f99ec8bbf899a1f/diff/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb95814/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Reported version : 1.1.1n
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1n
  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

2.9

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
overlay2/834484eb82b2041fa048b2a647874e9af27cb35ea471674c35c54e654f36dbdc/diff/lib/libcrypto.so.3
  Reported version : 3.0.8
  Fixed version    : 3.0.10
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
overlay2/834484eb82b2041fa048b2a647874e9af27cb35ea471674c35c54e654f36dbdc/diff/lib/libcrypto.so.3
  Reported version : 3.0.8
  Fixed version    : 3.0.13
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

5.9

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
overlay2/834484eb82b2041fa048b2a647874e9af27cb35ea471674c35c54e654f36dbdc/diff/lib/libcrypto.so.3
  Reported version : 3.0.8
  Fixed version    : 3.0.14
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/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

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/
overlay2/26b8a7831ae2152f932ab1eb03b6c3d7ff21b1d5d4ba2e3f6e253f421ecde6f5/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/
overlay2/834484eb82b2041fa048b2a647874e9af27cb35ea471674c35c54e654f36dbdc/diff/lib/libcrypto.so.3
  Reported version : 3.0.8
  Fixed version    : 3.0.9
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

187315 - SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Synopsis

The remote SSH server is vulnerable to a mitm prefix truncation attack.

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Note that this plugin only checks for remote SSH servers that support either ChaCha20-Poly1305 or CBC with Encrypt-then-MAC and do not support the strict key exchange countermeasures. It does not check for vulnerable software versions.

See Also

https://terrapin-attack.com/

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

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:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

6.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-48795

Plugin Information

Published: 2023/12/27, Modified: 2024/01/29

Plugin Output

tcp/22/ssh

```
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-etm@openssh.com
Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-64-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Server to Client algorithm  : hmac-sha1-etm@openssh.com
```

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
```

198044 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2 vulnerability (USN-6787-1)

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 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6787-1 advisory.

It was discovered that Jinja2 incorrectly handled certain HTML attributes that were accepted by the xmlattr filter. An attacker could use this issue to inject arbitrary HTML attribute keys and values to potentially execute a cross-site scripting (XSS) attack.

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-6787-1

Solution

Update the affected python-jinja2 and / or python3-jinja2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.3

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

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

References

CVE	CVE-2024-34064
XREF	USN:6787-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : python3-jinja2_3.0.3-1
  - Fixed package     : python3-jinja2_3.0.3-1ubuntu0.2
```

200307 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1)

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 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6827-1 advisory.

It was discovered that LibTIFF incorrectly handled memory when

performing certain cropping operations, leading to a heap buffer overflow. An attacker could use this issue to cause a

denial of service, or possibly execute arbitrary code.

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-6827-1

Solution

Update the affected packages.

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

3.6

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-2023-3164
XREF	USN:6827-1

Plugin Information

Published: 2024/06/11, Modified: 2024/06/11

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.9
```

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

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

  - Installed package : passwd_1:4.8.1-2ubuntu2.1
  - Fixed package     : passwd_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

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.
```

179893 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTIFF vulnerabilities (USN-6290-1)

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-6290-1 advisory.

- processCropSelections in tools/tiffcrop.c in LibTIFF through 4.5.0 has a heap-based buffer overflow (e.g., WRITE of size 307203) via a crafted TIFF image. (CVE-2022-48281)

- libtiff 4.5.0 is vulnerable to Buffer Overflow via /libtiff/tools/tiffcrop.c:8499. Incorrect updating of buffer size after rotateImage() in tiffcrop cause heap-buffer-overflow and SEGV. (CVE-2023-25433)

- loadImage() in tools/tiffcrop.c in LibTIFF through 4.5.0 has a heap-based use after free via a crafted TIFF image. (CVE-2023-26965)

- libtiff 4.5.0 is vulnerable to Buffer Overflow in uv_encode() when libtiff reads a corrupted little-endian TIFF file and specifies the output to be big-endian. (CVE-2023-26966)

- A NULL pointer dereference flaw was found in Libtiff's LZWDecode() function in the libtiff/tif_lzw.c file.

This flaw allows a local attacker to craft specific input data that can cause the program to dereference a NULL pointer when decompressing a TIFF format file, resulting in a program crash or denial of service.

(CVE-2023-2731)

- A null pointer dereference issue was found in Libtiff's tif_dir.c file. This issue may allow an attacker to pass a crafted TIFF image file to the tiffcp utility which triggers a runtime error that causes undefined behavior. This will result in an application crash, eventually leading to a denial of service.

(CVE-2023-2908)

- A NULL pointer dereference in TIFFClose() is caused by a failure to open an output file (non-existent path or a path that requires permissions like /dev/null) while specifying zones. (CVE-2023-3316)

- A flaw was found in libtiff. A specially crafted tiff file can lead to a segmentation fault due to a buffer overflow in the Fax3Encode function in libtiff/tif_fax3.c, resulting in a denial of service.

(CVE-2023-3618)

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-6290-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

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

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

References

CVE	CVE-2022-48281
CVE	CVE-2023-2731
CVE	CVE-2023-2908
CVE	CVE-2023-3316
CVE	CVE-2023-3618
CVE	CVE-2023-25433
CVE	CVE-2023-26965
CVE	CVE-2023-26966
CVE	CVE-2023-38288
CVE	CVE-2023-38289
XREF	USN:6290-1

Plugin Information

Published: 2023/08/16, Modified: 2023/08/16

Plugin Output

tcp/0

```

  - Installed package : libtiff5_4.3.0-6
```

```
    - Fixed package     : libtiff5_4.3.0-6ubuntu0.5
```

182891 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : LibTIFF vulnerability (USN-6428-1)

Synopsis

The remote Ubuntu host is missing a security update.

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 a vulnerability as referenced in the USN-6428-1 advisory.

- A flaw was found in tiffcrop, a program distributed by the libtiff package. A specially crafted tiff file can lead to an out-of-bounds read in the extractImageSection function in tools/tiffcrop.c, resulting in a denial of service and limited information disclosure. This issue affects libtiff versions 4.x.

(CVE-2023-1916)

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-6428-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.0

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-1916
XREF	USN:6428-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.6
```

189537 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.10 : Jinja2 vulnerabilities (USN-6599-1)

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 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6599-1 advisory.

- This affects the package jinja2 from 0.0.0 and before 2.11.3. The ReDoS vulnerability is mainly due to the `_punctuation_re regex` operator and its use of multiple wildcards. The last wildcard is the most exploitable as it searches for trailing punctuation. This issue can be mitigated by Markdown to format user content instead of the urlize filter, or by implementing request timeouts and limiting process memory. (CVE-2020-28493)

- Jinja is an extensible templating engine. Special placeholders in the template allow writing code similar to Python syntax. It is possible to inject arbitrary HTML attributes into the rendered HTML template, potentially leading to Cross-Site Scripting (XSS). The Jinja `xmlattr` filter can be abused to inject arbitrary HTML attribute keys and values, bypassing the auto escaping mechanism and potentially leading to XSS. It may also be possible to bypass attribute validation checks if they are blacklist-based.

(CVE-2024-22195)

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-6599-1

Solution

Update the affected python-jinja2 and / or python3-jinja2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.0

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)

References

CVE	CVE-2020-28493
CVE	CVE-2024-22195
XREF	USN:6599-1

Plugin Information

Published: 2024/01/25, Modified: 2024/01/25

Plugin Output

tcp/0

```
  - Installed package : python3-jinja2_3.0.3-1
  - Fixed package     : python3-jinja2_3.0.3-1ubuntu0.1
```

186225 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-6512-1)

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 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6512-1 advisory.

- An issue was discovered in function TIFFReadDirectory libtiff before 4.4.0 allows attackers to cause a denial of service via crafted TIFF file. (CVE-2022-40090)

- A memory leak flaw was found in Libtiff's tiffcrop utility. This issue occurs when tiffcrop operates on a TIFF image file, allowing an attacker to pass a crafted TIFF image file to tiffcrop utility, which causes this memory leak issue, resulting an application crash, eventually leading to a denial of service.

(CVE-2023-3576)

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-6512-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

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

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

References

CVE	CVE-2022-40090
CVE	CVE-2023-3576
XREF	USN:6512-1

Plugin Information

Published: 2023/11/23, Modified: 2023/11/23

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.7
```

168193 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : JBIG-KIT vulnerability (USN-5742-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 host has packages installed that are affected by a vulnerability as referenced in the USN-5742-1 advisory.

- In LibTIFF 4.0.8, there is a memory malloc failure in tif_jbig.c. A crafted TIFF document can lead to an abort resulting in a remote denial of service attack. (CVE-2017-9937)

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-5742-1

Solution

Update the affected jbigkit-bin, libjbig-dev and / or libjbig0 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

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

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

References

CVE	CVE-2017-9937
XREF	USN:5742-1

Plugin Information

Published: 2022/11/25, Modified: 2023/10/16

Plugin Output

tcp/0

```
  - Installed package : libjbig0_2.1-3.1build3
  - Fixed package     : libjbig0_2.1-3.1ubuntu0.22.04.1
```

165277 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5619-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5619-1 advisory.

- Buffer Overflow in LibTiff v4.0.10 allows attackers to cause a denial of service via the invertImage() function in the component tiffcrop. (CVE-2020-19131)

- Buffer Overflow in LibTiff v4.0.10 allows attackers to cause a denial of service via the 'in _TIFFmemcpy' funtion in the component 'tif_unix.c'. (CVE-2020-19144)

- A heap buffer overflow flaw was found in Libtiffs' tiffinfo.c in TIFFReadRawDataStriped() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffinfo tool, triggering a heap buffer overflow issue and causing a crash that leads to a denial of service. (CVE-2022-1354)

- A stack buffer overflow flaw was found in Libtiffs' tiffcp.c in main() function. This flaw allows an attacker to pass a crafted TIFF file to the tiffcp tool, triggering a stack buffer overflow issue, possibly corrupting the memory, and causing a crash that leads to a denial of service. (CVE-2022-1355)

- Divide By Zero error in tiffcrop in libtiff 4.4.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit f3a5e010.
(CVE-2022-2056, CVE-2022-2057, CVE-2022-2058)

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-5619-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.0

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)

References

CVE	CVE-2020-19131
CVE	CVE-2020-19144
CVE	CVE-2022-1354
CVE	CVE-2022-1355
CVE	CVE-2022-2056
CVE	CVE-2022-2057
CVE	CVE-2022-2058
XREF	USN:5619-1

Plugin Information

Published: 2022/09/21, Modified: 2023/07/12

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.1
```

167166 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5714-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5714-1 advisory.

- There is a double free or corruption in rotateImage() at tiffcrop.c:8839 found in libtiff 4.4.0rc1 (CVE-2022-2519)

- A flaw was found in libtiff 4.4.0rc1. There is a sysmalloc assertion fail in rotateImage() at tiffcrop.c:8621 that can cause program crash when reading a crafted input. (CVE-2022-2520)

- It was found in libtiff 4.4.0rc1 that there is an invalid pointer free operation in TIFFClose() at tif_close.c:131 called by tiffcrop.c:2522 that can cause a program crash and denial of service while processing crafted input. (CVE-2022-2521)

- libtiff's tiffcrop utility has a uint32_t underflow that can lead to out of bounds read and write. An attacker who supplies a crafted file to tiffcrop (likely via tricking a user to run tiffcrop on it with certain parameters) could cause a crash or in some cases, further exploitation. (CVE-2022-2867)

- libtiff's tiffcrop utility has a improper input validation flaw that can lead to out of bounds read and ultimately cause a crash if an attacker is able to supply a crafted file to tiffcrop. (CVE-2022-2868)

- libtiff's tiffcrop tool has a uint32_t underflow which leads to out of bounds read and write in the extractContigSamples8bits routine. An attacker who supplies a crafted file to tiffcrop could trigger this flaw, most likely by tricking a user into opening the crafted file with tiffcrop. Triggering this flaw could cause a crash or potentially further exploitation. (CVE-2022-2869)

- LibTIFF 4.4.0 has an out-of-bounds read in extractImageSection in tools/tiffcrop.c:6905, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 48d6ece8. (CVE-2022-2953)

- Multiple heap buffer overflows in tiffcrop.c utility in libtiff library Version 4.4.0 allows attacker to trigger unsafe or out of bounds memory access via crafted TIFF image file which could result into application crash, potential information disclosure or any other context-dependent impact (CVE-2022-3570)

- LibTIFF 4.4.0 has an out-of-bounds write in extractContigSamplesShifted24bits in tools/tiffcrop.c:3604, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit cfbb883b. (CVE-2022-3598)

- LibTIFF 4.4.0 has an out-of-bounds read in writeSingleSection in tools/tiffcrop.c:7345, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit e8131125. (CVE-2022-3599)

- LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemset in libtiff/tif_unix.c:340 when called from processCropSelections, tools/tiffcrop.c:7619, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191.

(CVE-2022-3626)

- LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemcpy in libtiff/tif_unix.c:346 when called from extractImageSection, tools/tiffcrop.c:6860, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191.

(CVE-2022-3627)

- A stack overflow was discovered in the _TIFFVGetField function of Tiffsplit v4.4.0. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted TIFF file. (CVE-2022-34526)

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-5714-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

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

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

References

CVE	CVE-2022-2519
CVE	CVE-2022-2520
CVE	CVE-2022-2521
CVE	CVE-2022-2867

CVE	CVE-2022-2868
CVE	CVE-2022-2869
CVE	CVE-2022-2953
CVE	CVE-2022-3570
CVE	CVE-2022-3597
CVE	CVE-2022-3598
CVE	CVE-2022-3599
CVE	CVE-2022-3626
CVE	CVE-2022-3627
CVE	CVE-2022-34526
XREF	USN:5714-1

Plugin Information

Published: 2022/11/09, Modified: 2023/10/16

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.2
```

172213 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS : LibTIFF vulnerabilities (USN-5923-1)

Synopsis

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

Description

The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 22.04 LTS / 22.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5923-1 advisory.

- LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3488, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e. (CVE-2023-0795)

- LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3592, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e. (CVE-2023-0796)

- LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in libtiff/tif_unix.c:368, invoked by tools/tiffcrop.c:2903 and tools/tiffcrop.c:6921, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e.

(CVE-2023-0797)

- LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3400, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e. (CVE-2023-0798)

- LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3701, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit afaabc3e. (CVE-2023-0799)

- LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3502, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127. (CVE-2023-0800)

- LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in libtiff/tif_unix.c:368, invoked by tools/tiffcrop.c:2903 and tools/tiffcrop.c:6778, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127.

(CVE-2023-0801)

- LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3724, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127. (CVE-2023-0802)

- LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3516, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127. (CVE-2023-0803)

- LibTIFF 4.4.0 has an out-of-bounds write in tiffcrop in tools/tiffcrop.c:3609, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 33aee127. (CVE-2023-0804)

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-5923-1

Solution

Update the affected packages.

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

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

VPR Score

4.4

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

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

References

CVE	CVE-2023-0795
CVE	CVE-2023-0796
CVE	CVE-2023-0797
CVE	CVE-2023-0798
CVE	CVE-2023-0799
CVE	CVE-2023-0800
CVE	CVE-2023-0801
CVE	CVE-2023-0802
CVE	CVE-2023-0803
CVE	CVE-2023-0804
XREF	USN:5923-1

Plugin Information

Published: 2023/03/07, Modified: 2023/10/16

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.4
```

197569 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 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-6780-1 advisory.

Guido Vranken discovered that idna did not properly manage certain inputs,

which could lead to significant resource consumption. 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-6780-1

Solution

Update the affected pypy-idna, python-idna and / or python3-idna 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:N/I:N/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-3651
XREF	USN:6780-1

Plugin Information

Published: 2024/05/21, Modified: 2024/05/23

Plugin Output

tcp/0

```
  - Installed package : python3-idna_3.3-1
  - Fixed package     : python3-idna_3.3-1ubuntu0.1
```

191637 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : c-ares vulnerability (USN-6676-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 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-6676-1 advisory.

- c-ares is a C library for asynchronous DNS requests. `ares__read_line()` is used to parse local configuration files such as `/etc/resolv.conf`, `/etc/nsswitch.conf`, the `HOSTALIASES` file, and if using a c-ares version prior to 1.27.0, the `/etc/hosts` file. If any of these configuration files has an embedded `NULL` character as the first character in a new line, it can lead to attempting to read memory prior to the start of the given buffer which may result in a crash. This issue is fixed in c-ares 1.27.0.

No known workarounds exist. (CVE-2024-25629)

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-6676-1

Solution

Update the affected libc-ares-dev and / or libc-ares2 packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-25629
XREF	USN:6676-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : libc-ares2_1.18.1-1build1
  - Fixed package     : libc-ares2_1.18.1-1ubuntu0.22.04.3
```

186084 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : GnuTLS vulnerability (USN-6499-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6499-1 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-6499-1

Solution

Update the affected packages.

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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-5981

XREF USN:6499-1

Plugin Information

Published: 2023/11/21, Modified: 2023/12/05

Plugin Output

tcp/0

```
  - Installed package : libgnutls30_3.7.3-4ubuntu1.2
  - Fixed package     : libgnutls30_3.7.3-4ubuntu1.3
```

189143 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : PAM vulnerability (USN-6588-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6588-1 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-6588-1

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: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

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-2024-22365

XREF USN:6588-1

Plugin Information

Published: 2024/01/17, Modified: 2024/02/14

Plugin Output

tcp/0

```
  - Installed package : libpam-modules_1.4.0-11ubuntu2.3
  - Fixed package     : libpam-modules_1.4.0-11ubuntu2.4

  - Installed package : libpam-modules-bin_1.4.0-11ubuntu2.3
  - Fixed package     : libpam-modules-bin_1.4.0-11ubuntu2.4

  - Installed package : libpam-runtime_1.4.0-11ubuntu2.3
  - Fixed package     : libpam-runtime_1.4.0-11ubuntu2.4

  - Installed package : libpam0g_1.4.0-11ubuntu2.3
  - Fixed package     : libpam0g_1.4.0-11ubuntu2.4
```

187918 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Twisted vulnerabilities (USN-6575-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6575-1 advisory.

- Twisted is an event-based framework for internet applications. Started with version 0.9.4, when the host header does not match a configured host `twisted.web.vhost.NameVirtualHost` will return a `NoResource` resource which renders the Host header unescaped into the 404 response allowing HTML and script injection.

In practice this should be very difficult to exploit as being able to modify the Host header of a normal HTTP request implies that one is already in a privileged position. This issue was fixed in version 22.10.0rc1. There are no known workarounds. (CVE-2022-39348)

- Twisted is an event-based framework for internet applications. Prior to version 23.10.0rc1, when sending multiple HTTP requests in one TCP packet, twisted.web will process the requests asynchronously without guaranteeing the response order. If one of the endpoints is controlled by an attacker, the attacker can delay the response on purpose to manipulate the response of the second request when a victim launched two requests using HTTP pipeline. Version 23.10.0rc1 contains a patch for this issue. (CVE-2023-46137)

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-6575-1

Solution

Update the affected python3-twisted and / or python3-twisted-bin packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.8

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2022-39348
CVE	CVE-2023-46137
XREF	USN:6575-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : python3-twisted_22.1.0-2ubuntu2.3
  - Fixed package     : python3-twisted_22.1.0-2ubuntu2.4
```

186615 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : curl vulnerabilities (USN-6535-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6535-1 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-6535-1

Solution

Update the affected packages.

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

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)

STIG Severity

I

References

CVE	CVE-2023-46218
CVE	CVE-2023-46219
XREF	USN:6535-1
XREF	IAVA:2023-A-0674-S

Plugin Information

Published: 2023/12/06, Modified: 2024/02/02

Plugin Output

tcp/0

```
  - Installed package : curl_7.81.0-1ubuntu1.14
  - Fixed package     : curl_7.81.0-1ubuntu1.15

  - Installed package : libcurl3-gnutls_7.81.0-1ubuntu1.14
  - Fixed package     : libcurl3-gnutls_7.81.0-1ubuntu1.15

  - Installed package : libcurl4_7.81.0-1ubuntu1.14
  - Fixed package     : libcurl4_7.81.0-1ubuntu1.15
```

189295 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libssh vulnerabilities (USN-6592-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6592-1 advisory.

- A flaw was found in libssh. By utilizing the ProxyCommand or ProxyJump feature, users can exploit unchecked hostname syntax on the client. This issue may allow an attacker to inject malicious code into the command of the features mentioned through the hostname parameter. (CVE-2023-6004)

- A flaw was found in the libssh implements abstract layer for message digest (MD) operations implemented by different supported crypto backends. The return values from these were not properly checked, which could cause low-memory situations failures, NULL dereferences, crashes, or usage of the uninitialized memory as an input for the KDF. In this case, non-matching keys will result in decryption/ integrity failures, terminating the connection. (CVE-2023-6918)

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-6592-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.2

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-6004
CVE	CVE-2023-6918
XREF	USN:6592-1

Plugin Information

Published: 2024/01/22, Modified: 2024/01/22

Plugin Output

tcp/0

```
  - Installed package : libssh-4_0.9.6-2ubuntu0.22.04.1
  - Fixed package     : libssh-4_0.9.6-2ubuntu0.22.04.3

  - Installed package : libssh-gcrypt-4_0.9.6-2build1
  - Fixed package     : libssh-gcrypt-4_0.9.6-2ubuntu0.22.04.3
```

187106 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : libssh vulnerability (USN-6561-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6561-1 advisory.

- The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD 1.3.9rc1, ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust; and there could be effects on Bitvise SSH through 9.31. (CVE-2023-48795)

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-6561-1

Solution

Update the affected packages.

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:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

6.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2023-48795
XREF	USN:6561-1
XREF	IAVA:2023-A-0703

Plugin Information

Published: 2023/12/19, Modified: 2023/12/29

Plugin Output

tcp/0

```
  - Installed package : libssh-4_0.9.6-2ubuntu0.22.04.1
  - Fixed package     : libssh-4_0.9.6-2ubuntu0.22.04.2

  - Installed package : libssh-gcrypt-4_0.9.6-2build1
  - Fixed package     : libssh-gcrypt-4_0.9.6-2ubuntu0.22.04.2
```

186623 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : python-cryptography vulnerabilities (USN-6539-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6539-1 advisory.

- cryptography is a package designed to expose cryptographic primitives and recipes to Python developers. In affected versions `Cipher.update_into` would accept Python objects which implement the buffer protocol, but provide only immutable buffers. This would allow immutable objects (such as `bytes`) to be mutated, thus violating fundamental rules of Python and resulting in corrupted output. This now correctly raises an exception. This issue has been present since `update_into` was originally introduced in cryptography 1.8.

(CVE-2023-23931)

- cryptography is a package designed to expose cryptographic primitives and recipes to Python developers.

Calling `load_pem_pkcs7_certificates` or `load_der_pkcs7_certificates` could lead to a NULL-pointer dereference and segfault. Exploitation of this vulnerability poses a serious risk of Denial of Service (DoS) for any application attempting to deserialize a PKCS7 blob/certificate. The consequences extend to potential disruptions in system availability and stability. This vulnerability has been patched in version 41.0.6. (CVE-2023-49083)

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-6539-1

Solution

Update the affected python-cryptography and / or python3-cryptography packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-23931
CVE	CVE-2023-49083
XREF	USN:6539-1

Plugin Information

Published: 2023/12/06, Modified: 2023/12/06

Plugin Output

tcp/0

```
  - Installed package : python3-cryptography_3.4.8-1ubuntu2
  - Fixed package     : python3-cryptography_3.4.8-1ubuntu2.1
```

184451 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Kerberos vulnerability (USN-6467-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6467-2 advisory.

- lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count. (CVE-2023-36054)

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-6467-2

Solution

Update the affected 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:N/I:N/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-36054
XREF	USN:6467-2

Plugin Information

Published: 2023/11/06, Modified: 2023/11/06

Plugin Output

tcp/0

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

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

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

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

186307 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : Python vulnerability (USN-6513-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.04 host has packages installed that are affected by a vulnerability as referenced in the USN-6513-2 advisory.

- An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) that use TLS client authentication. If a TLS server-side socket is created, receives data into the socket buffer, and then is closed quickly, there is a brief window where the SSLSocket instance will detect the socket as not connected and won't initiate a handshake, but buffered data will still be readable from the socket buffer. This data will not be authenticated if the server-side TLS peer is expecting client certificate authentication, and is indistinguishable from valid TLS stream data. Data is limited in size to the amount that will fit in the buffer. (The TLS connection cannot directly be used for data exfiltration because the vulnerable code path requires that the connection be closed on initialization of the SSLSocket.) (CVE-2023-40217)

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-6513-2

Solution

Update the affected packages.

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

1.4

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)

References

CVE	CVE-2023-40217
XREF	USN:6513-2

Plugin Information

Published: 2023/11/27, Modified: 2023/11/27

Plugin Output

tcp/0

```

  - Installed package : libpython3.10_3.10.12-1~22.04.2
  - Fixed package     : libpython3.10_3.10.12-1~22.04.3

  - Installed package : libpython3.10-minimal_3.10.12-1~22.04.2
  - Fixed package     : libpython3.10-minimal_3.10.12-1~22.04.3

  - Installed package : libpython3.10-stdlib_3.10.12-1~22.04.2
  - Fixed package     : libpython3.10-stdlib_3.10.12-1~22.04.3

  - Installed package : python3.10_3.10.12-1~22.04.2
  - Fixed package     : python3.10_3.10.12-1~22.04.3

  - Installed package : python3.10-minimal_3.10.12-1~22.04.2
  - Fixed package     : python3.10-minimal_3.10.12-1~22.04.3

```

177324 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : c-ares vulnerabilities (USN-6164-1)

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-6164-1 advisory.

- c-ares is an asynchronous resolver library. ares_inet_net_pton() is vulnerable to a buffer underflow for certain ipv6 addresses, in particular 0::00:00:00/2 was found to cause an issue. C-ares only uses this function internally for configuration purposes which would require an administrator to configure such an address via ares_set_sortlist(). However, users may externally use ares_inet_net_pton() for other purposes and thus be vulnerable to more severe issues. This issue has been fixed in 1.19.1. (CVE-2023-31130)

- c-ares is an asynchronous resolver library. c-ares is vulnerable to denial of service. If a target resolver sends a query, the attacker forges a malformed UDP packet with a length of 0 and returns them to the target resolver. The target resolver erroneously interprets the 0 length as a graceful shutdown of the connection. This issue has been patched in version 1.19.1. (CVE-2023-32067)

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-6164-1

Solution

Update the affected libc-ares-dev and / or libc-ares2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

CVSS v2.0 Base Score

5.9 (CVSS2#AV:L/AC:H/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-31130
CVE	CVE-2023-32067
XREF	USN:6164-1

Plugin Information

Published: 2023/06/14, Modified: 2023/10/20

Plugin Output

tcp/0

```
  - Installed package : libc-ares2_1.18.1-1build1
  - Fixed package     : libc-ares2_1.18.1-1ubuntu0.22.04.2
```

176712 - Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : libssh vulnerabilities (USN-6138-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 22.10 / 23.04 host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6138-1 advisory.

- A NULL pointer dereference was found In libssh during re-keying with algorithm guessing. This issue may allow an authenticated client to cause a denial of service. (CVE-2023-1667)

- A vulnerability was found in libssh, where the authentication check of the connecting client can be bypassed in the`pki_verify_data_signature` function in memory allocation problems. This issue may happen if there is insufficient memory or the memory usage is limited. The problem is caused by the return value `rc,` which is initialized to SSH_ERROR and later rewritten to save the return value of the function call `pki_key_check_hash_compatible.` The value of the variable is not changed between this point and the cryptographic verification. Therefore any error between them calls `goto error` returning SSH_OK.

(CVE-2023-2283)

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-6138-1

Solution

Update the affected packages.

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

3.6

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)

STIG Severity

II

References

CVE	CVE-2023-1667
CVE	CVE-2023-2283
XREF	USN:6138-1
XREF	IAVA:2023-A-0517-S

Plugin Information

Published: 2023/06/05, Modified: 2023/12/22

Plugin Output

tcp/0

```
  - Installed package : libssh-gcrypt-4_0.9.6-2build1
  - Fixed package     : libssh-gcrypt-4_0.9.6-2ubuntu0.22.04.1
```

198063 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : TPM2 Software Stack vulnerabilities (USN-6796-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6796-1 advisory.

Fergus Dall discovered that TPM2 Software Stack did not properly handle layer arrays. An attacker could possibly use this issue to cause

TPM2 Software Stack to crash, resulting in a denial of service, or

possibly execute arbitrary code. (CVE-2023-22745)

Jurgen Repp and Andreas Fuchs discovered that TPM2 Software Stack did not

validate the quote data after deserialization. An attacker could generate an arbitrary quote and cause TPM2 Software Stack to have unknown behavior.

(CVE-2024-29040)

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-6796-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

5.9 (CVSS2#AV:L/AC:H/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22745
CVE	CVE-2024-29040
XREF	USN:6796-1

Plugin Information

Published: 2024/05/29, Modified: 2024/05/29

Plugin Output

tcp/0

```
  - Installed package : libtss2-esys-3.0.2-0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-esys-3.0.2-0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-mu0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-mu0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-sys1_3.2.0-1ubuntu1
  - Fixed package     : libtss2-sys1_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-cmd0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-cmd0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-device0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-device0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-mssim0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-mssim0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-swtpm0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-swtpm0_3.2.0-1ubuntu1.1
```

194475 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU cpio vulnerabilities (USN-6755-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6755-1 advisory.

- Debian's cpio contains a path traversal vulnerability. This issue was introduced by reverting CVE-2015-1197 patches which had caused a regression in --no-absolute-filenames. Upstream has since provided a proper fix to --no-absolute-filenames. (CVE-2023-7207)

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-6755-1

Solution

Update the affected cpio and / or cpio-win32 packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-7207
XREF	USN:6755-1

Plugin Information

Published: 2024/04/29, Modified: 2024/04/29

Plugin Output

tcp/0

```
  - Installed package : cpio_2.13+dfsg-7
  - Fixed package     : cpio_2.13+dfsg-7ubuntu0.1
```

193341 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GnuTLS vulnerabilities (USN-6733-1)

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-6733-1 advisory.

- A flaw was found in GnuTLS. The Minerva attack is a cryptographic vulnerability that exploits deterministic behavior in systems like GnuTLS, leading to side-channel leaks. In specific scenarios, such as when using the GNUTLS_PRIVKEY_FLAG_REPRODUCIBLE flag, it can result in a noticeable step in nonce size from 513 to 512 bits, exposing a potential timing side-channel. (CVE-2024-28834)

- A flaw has been discovered in GnuTLS where an application crash can be induced when attempting to verify a specially crafted .pem bundle using the certtool --verify-chain command. (CVE-2024-28835)

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-6733-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28834
CVE	CVE-2024-28835
XREF	USN:6733-1

Plugin Information

Published: 2024/04/15, Modified: 2024/04/15

Plugin Output

tcp/0

```
  - Installed package : libgnutls30_3.7.3-4ubuntu1.2
  - Fixed package     : libgnutls30_3.7.3-4ubuntu1.5
```

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

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
```

189992 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : OpenSSL vulnerabilities (USN-6622-1)

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-6622-1 advisory.

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

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

- 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: 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. Found by OSS-Fuzz. Fix developed by Tomas Mraz. Fixed in OpenSSL 3.0.13 (Affected since 3.0.0). (CVE-2023-6237)

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-6622-1

Solution

Update the affected packages.

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

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	USN:6622-1
XREF	IAVA:2024-A-0121-S

Plugin Information

Published: 2024/02/05, Modified: 2024/04/11

Plugin Output

tcp/0

```
  - Installed package : libssl3_3.0.2-0ubuntu1.10
  - Fixed package     : libssl3_3.0.2-0ubuntu1.14

  - Installed package : openssl_3.0.2-0ubuntu1.10
  - Fixed package     : openssl_3.0.2-0ubuntu1.14
```

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

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

6.7

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.
```

185569 - Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : procps-ng vulnerability (USN-6477-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6477-1 advisory.

- Under some circumstances, this weakness allows a user who has access to run the ps utility on a machine, the ability to write almost unlimited amounts of unfiltered data into the process heap. (CVE-2023-4016)

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-6477-1

Solution

Update the affected packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

1.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

II

References

CVE	CVE-2023-4016
XREF	IAVA:2023-A-0434
XREF	USN:6477-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : libprocps8_2:3.3.17-6ubuntu2
  - Fixed package     : libprocps8_2:3.3.17-6ubuntu2.1

  - Installed package : procps_2:3.3.17-6ubuntu2
  - Fixed package     : procps_2:3.3.17-6ubuntu2.1
```

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

2.2

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              : /snap/lxd/24322/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.6.0
  Installed version : 7.68.0
  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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 3 installs of Apache Log4j:

  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

  Path                              : /usr/share/apport/testsuite/crash.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/apport/apport.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: 2024/06/24

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:24.0.6 -> Docker
  cpe:/a:gnupg:libgcrypt:1.8.5 -> GnuPG Libgcrypt
  cpe:/a:gnupg:libgcrypt:1.8.8 -> GnuPG Libgcrypt
  cpe:/a:gnupg:libgcrypt:1.9.4 -> GnuPG Libgcrypt
  cpe:/a:haxx:curl:7.81.0 -> Haxx Curl
  cpe:/a:haxx:libcurl:7.68.0 -> Haxx libcurl
  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:1.1.1f -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:1.1.1k -> OpenSSL Project OpenSSL
```

```
    cpe:/a:openssl:openssl:1.1.1n -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:3.0.2 -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:3.0.8 -> OpenSSL Project OpenSSL
    cpe:/a:sqlite:sqlite -> SQLite
    cpe:/a:tukaani:xz -> Tukaani XZ
    cpe:/a:tukaani:xz:5.0.0 -> Tukaani XZ
    cpe:/a:tukaani:xz:5.2.4 -> Tukaani XZ
    cpe:/a:tukaani:xz:5.2.5 -> Tukaani XZ
    cpe:/a:tukaani:xz:5.2.9 -> Tukaani XZ
    cpe:/a:vim:vim:8.1 -> Vim
    cpe:/a:vim:vim:8.2 -> Vim
    cpe:/a:vmware:open_vm_tools:12.1.5 -> VMware Open VM Tools
```

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: 2024/06/24

Plugin Output

tcp/0

```
Path               : /usr/bin/curl
Version            : 7.81.0
Associated Package : curl 7.81.0-1ubuntu1.14
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: 2024-06-26 08:49:23
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: 2024/06/24

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: 2024/06/24

Plugin Output

tcp/0

```
Docker container b9cfa149a1001de58f5cb288df8def4d3da4a6a9eb4c9c455feb3f902fc59f1d has 9 changed
 files

Docker container cfc0a0741fbcf907c08ffcaf49d1115f1de24c275442ec6b9c065d188c34093f has 3 changed
 files

Docker container e2e3352340491739d9c89a2bf84a9a4e2c3c24fd22b7c7a55dd867d8ca9ef912 has 20 changed
 files

Docker container 6b9c3f76b6433573b9ddccebb7b3932b8560ca8a31fcace6514e72f7b87447be has 14 changed
 files

Docker container 859a9f5db7b21813f3cc9e2990d9523bff01b76cb5456f00e97ec50ae00686ae has 7 changed
 files

Docker container d9d3bed7a3c19c8a39415b95f6ca1bd989d860eb24becfcebceebbc9eb31e3dc has 6 changed
 files

Docker container 91741ed3962cd10d83d7308d56c52c6b7823396b7c68960b57d7bcfad17957cb has 26 changed
 files

Docker container 80d62083b1cb1e1d7d6ae5e5a0a987f7ef948648f71f73b00a1bdce38eab2143 has 6 changed
 files
```

```
Docker container 2b95b5296ff7abc5cf8b45d7b013c16a20c8ddc41798fb7803ede30f9fc5cfe6 has 6 changed
 files

Docker container 90c48bbe15145b371e5967bfdec67cb6d5f8f16ee469f9b4a4f70e12c8e5d996 has 5 changed
 files

Docker container 8419392efc1293ce174c3042a284469ec9fa8659d4d094ee7d910f66b4d358dc 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: 2024/06/24

Plugin Output

tcp/0

```
  Path    : /usr/bin/docker
  Version : 24.0.6
  build   : ed223bc
```

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: 2024/06/24

Plugin Output

tcp/0

```
  Version: 24.0.6
  Version: 24.0.6
  Version: 1.6.24
  Version: 1.1.9
  Version: 0.19.0

The following containers were detected running on the remote Docker host :

Name:      /appliance-cron
Image:     appliance
Image ID : sha256:ba7db42bff63c74a42b7b91d11f4cc8dcb673c763818b650ee22cd0a3594e046
Tag:       v0.34.1
ID:        b9cfa149a1001de58f5cb288df8def4d3da4a6a9eb4c9c455feb3f902fc59f1d
Ports:     n/a

Name:      /telemetry
Image:     opentelemetry-collector
Image ID : sha256:89ad870fc4b7fe394df5973eda1c551b7244d4f746710a5a634b75e35360bea5
Tag:       v0.34.1
ID:        cfc0a0741fbcf907c08ffcaf49d1115f1de24c275442ec6b9c065d188c34093f
Ports:     n/a

Name:      /dataplane
Image:     vpp-dataplane
```

```
Image ID : sha256:63349f0ad38984e2692d37a185cd6d89ec72e14c96822c591c22d4910eb32148
Tag:       v0.34.1
ID:        e2e3352340491739d9c89a2bf84a9a4e2c3c24fd22b7c7a55dd867d8ca9ef912
Ports:     n/a

Name:      /daemon-64-2_0_2c
Image:     scion-all
Image ID : sha256:8707599aa6d1e924d4c7baecfb1b9c0e408292440be7260221bfd49476eda8c3
Tag:       v0.34.1
ID:        6b9c3f76b6433573b9ddccebb7b3932b8560ca8a31fcace6514e72f7b87447be
Ports:     n/a

Name:      /dataplane-control
Image:     scion-all
Image ID : sha256:8707599aa6d1e924d4c7baecfb1b9c0e408292440be7260221bfd49476eda8c3
Tag:       v0.34.1
ID:        859a9f5db7b21813f3cc9e2990d9523bff01b76cb5456f00e97ec50ae00686ae
Ports:     n/a

Name:      /router
Image:     scion-all
Image ID : sha256:8707599aa6d1e924d4c7baecfb1b9c0e408292440be7260221bfd49476eda8c3
Tag:       v0.34.1
ID:        d9d3bed7a3c19c8a39415b95f6ca1bd989d860eb24becfcebceebbc9eb31e3dc
Ports:     n/a

Name:      /control-64-2_0_2c
Image:     scion-all
Image ID : sha256:8707599aa6d1e924d4c7baecfb1b9c0e408292440be7260221bfd49476eda8c3
Tag:       v0.34.1
ID:        91741ed3962cd10d83d7308d56c52c6b7823396b7c68960b57d7bcfad17957cb
Ports:     n/a

Name:      /gateway
Image:     scion-all
Image ID : sha256:8707599aa6d1e924d4c7baecfb1b9c0e408292440be7260221bfd49476eda8c3
Tag:       v0.34.1
ID:        80d62083b1cb1e1d7d6a [...]
```

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::f165:8622:2522:ecde (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::f165:8622:2522:ecde
        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
     - 31.10.193.176/30
     - 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
     - 46.140.142.96/29
     - 46.140.148.112/28
     - 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
     - 84.226.0.0/1 [...]
```

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: 2024/06/24

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: 2021/05/19

Plugin Output

tcp/443/www

```

  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: Wed, 26 Jun 2024 08:50:10 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: Wed, 26 Jun 2024 08:50:10 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: 2024/06/24

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::f165:8622:2522:ecde
        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: 2024/06/24

Plugin Output

tcp/0

```
JAR files found: 3
 - /usr/share/java/libintl-0.21.jar
 - /usr/share/apport/apport.jar
 - /usr/share/apport/testsuite/crash.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: 2024/06/24

Plugin Output

tcp/0

```

Nessus detected 18 installs of Libgcrypt:

  Path    : /snap/core20/1974/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.8.5

  Path    : /snap/core20/1974/lib/x86_64-linux-gnu/libgcrypt.so.20.2.5
  Version : 1.8.5

  Path    : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.8.5

  Path    : /snap/core20/1974/usr/lib/x86_64-linux-gnu/libgcrypt.so.20.2.5
  Version : 1.8.5

  Path    : /snap/core20/current/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.8.5

  Path    : /snap/core20/current/lib/x86_64-linux-gnu/libgcrypt.so.20.2.5
  Version : 1.8.5

  Path    : /snap/core20/current/usr/lib/x86_64-linux-gnu/libgcrypt.so.20
  Version : 1.8.5

  Path    : /snap/core20/current/usr/lib/x86_64-linux-gnu/libgcrypt.so.20.2.5
  Version : 1.8.5

  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    : /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/VP7BNNTX76GBD6OM2ME7G5N5E6/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/l/VP7BNNTX76GBD6OM2ME7G5N5E6/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /usr/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
```

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  3.3M  3.1G   1% /run
/dev/mapper/vg--main-lv--root      219G   13G  196G   6% /
tmpfs                               16G     0   16G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          406M  130M  244M  35% /boot
/dev/mapper/vg--secondary-lv--var  219G  7.7G  201G   4% /var
/dev/sda1                          127M  6.1M  120M   5% /boot/efi
overlay                            219G  7.7G  201G   4% /var/lib/docker/
overlay2/0c76b5b0d25455f0eb98841db9773ada467e7a3a51b207d49814636f4d191bf3/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/overlay2/
bfefc375cf29ddecd923cfc6b98eb1a99113819db8a7322a4e631d1a8ba4362e/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/overlay2/
a3d0cc30e6d655d2bc580fe658ce4247f74f875cf6566a92717a60d5354e2a62/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/
overlay2/1f2fe32f63853204187a370c752e9a2e6a872018fd4b61ac86297ef0a1689bf2/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged
```

```
overlay                            219G  7.7G  201G   4% /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged
overlay                            219G  7.7G  201G   4% /var/lib/docker/
overlay2/9fddca3e5e015b31c6577e71e9cf95af31d0c1893eceb91fccb6ae534eb [...]
```

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: UTC (UTC, +0000)
Via /etc/timezone: 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: 2024/06/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202406250936
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1404-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 : 211.135 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 : 2024/6/26 10:47 CEST
Scan duration : 1270 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: 2024/06/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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 daemon is not managed by dpkg :

/usr/local/bin/appliance
```

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 : 24.952863 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: 2024/06/24

Plugin Output

tcp/22/ssh

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

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: 2024/06/24

Plugin Output

tcp/0

```

Nessus detected 41 installs of OpenSSL:

  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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Version : 1.1.1n

  Path    : /snap/core20/1974/usr/bin/openssl
  Version : 1.1.1f

  Path    : /var/lib/docker/overlay2/
c0847f4bed1e046e5e68dd6126b56bc1e375255ed2cd2535ee5dd9df7bab4074/merged/usr/bin/openssl
```

```
  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/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/usr/bin/openssl
  Version : 1.1.1n

  Path    : /var/lib/docker/overlay2/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  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/
a76eaa1a4f558bf27c7792a944c0397914d2a77e3e5a5e0de7d348f0b749fc7c/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
cc789001a1b6e2b35caf923e9c83162cad423aec3df9039ac9ce1e950cf852b3/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/67025052915f5c9ff8fba827a2f55e2f861ff6962e5f093b8d8121fc2aa8829d/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Version : 1.1.1k

  Path    : /v [...]
```

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: 2024/06/11

Plugin Output

tcp/0

```

. You need to take the following 81 actions :


[ OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities (192965) ]

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

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).



[ OpenSSL 3.0.0 < 3.0.14 Multiple Vulnerabilities (192966) ]

+ Action to take : Upgrade to OpenSSL version 3.0.14 or later.

+Impact : Taking this action will resolve 45 different vulnerabilities (CVEs).



[ SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795) (187315) ]

+ Action to take : Contact the vendor for an update with the strict key exchange countermeasures or
 disable the affected algorithms.
```

```
[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2
 vulnerability (USN-6787-1) (198044) ]

+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF
 vulnerability (USN-6827-1) (200307) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less
 vulnerability (USN-6756-1) (194474) ]

+ Action to take : Update the affected less package.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability
 (USN-6698-1) (192219) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities
 (USN-6736-1) (193362) ]

+ Action to take : Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

+Impact : Taking this action will resolve 4 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 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)
 (185568) ]

+ Action to take : Update t [...]
```

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
```

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

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

Solution

Disable IPv6 if you do not actually using it.

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```

The following global addresss were gathered :

  - ['ipv6': fe80::3eec:efff:fede:9ac4]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': fe80::f165:8622:2522:ecde]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': ::1]['scope': host]['scopeid': 0x10]['prefixlen': 128]
  - ['ipv6': fe80::3eec:efff:fede:9d5f]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': fe80::3eec:efff:fede:9d5e]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': fe80::3eec:efff:fede:9ac5]['scope': link]['scopeid': 0x20]['prefixlen': 64]
```

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: 2023/11/27

Plugin Output

tcp/22/ssh

```
Process ID   : 1146655
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: 2023/11/27

Plugin Output

tcp/80

```
  Process ID   : 1514
  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: 2023/11/27

Plugin Output

tcp/443/www

```
  Process ID   : 1514
  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: 2023/11/27

Plugin Output

udp/443

```
  Process ID   : 1514
  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: 2023/11/27

Plugin Output

udp/30041

```
  Process ID   : 2419
  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: 2023/11/27

Plugin Output

udp/30042

```
  Process ID   : 1358247
  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: 2023/11/27

Plugin Output

tcp/30252

```
  Process ID   : 2458
  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: 2023/11/27

Plugin Output

tcp/42001/www

```

  Process ID   : 1514
  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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 5 installs of SQLite:

  Path    : /snap/core20/1974/usr/share/bash-completion/completions/sqlite3
  Version : unknown

  Path    : /snap/core20/current/usr/share/bash-completion/completions/sqlite3
  Version : unknown

  Path    : /snap/lxd/24322/bin/sqlite3
  Version : unknown

  Path    : /snap/lxd/current/bin/sqlite3
  Version : unknown

  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
  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: 2021/01/19

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: 2023/11/27

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: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3
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 : Jul 02 11:44:25 2024 GMT

|-Subject   :
|-Not After : Jun 26 18:38:10 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
Jun 26 18:38:10 2024 GMT :

  Subject          : n/a
  Issuer           : CN=Caddy Local Authority - ECC Intermediate
  Not valid before : Jun 26 06:38:10 2024 GMT
  Not valid after  : Jun 26 18:38:10 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: 4F 5F 1B 60 1F 9D ED BA 7C 7C EF C1 F4 2A 0F E7

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:38:10 2024 GMT
Not Valid After: Jun 26 18:38:10 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 06 56 D3 96 CE 6B 21 8A CF C8 40 95 C8 78 66 4A 29 8C 3F 8D
              D1 39 1F E1 9D CE 1C 2E 60 C6 77 6F
Public Key Y: 58 D6 1B D8 5F 07 5B CF A0 D9 04 9B 7C E0 93 38 E0 D5 12 C4
              EB 33 0F E6 AC CF 29 8C 3F 06 C2 51

Signature Length: 72 bytes / 576 bits
Signature: 00 30 46 02 21 00 B8 65 36 08 5A 0B DE 52 B1 92 C0 ED 83 59
           94 7B 29 18 D2 11 5F 8F A1 1A CA 7C 63 32 84 D1 FD 1B 02 21
           00 A2 7C 16 3C 8F 32 FD 7C 48 F4 D5 14 36 10 0B AB 30 06 FA
           2C C2 72 3D 4E 33 D6 64 01 88 C5 41 BD
```

```
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: 06 85 F0 00 D4 F1 9A 13 96 13 9F A6 E3 6D 9F 5A 97 66 E6 1D


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: FB 63 D0 CB 34 45 D8 8A C0 57 3A 13 79 75 51 7A B4 DB 95 DB


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1


Fingerprints :

SHA-256 Fingerprint: 62 EF 46 BC 80 25 24 96 76 90 E6 C4 97 78 9C E2 6F CF 97 43
                     CD 53 AD E3 89 85 A4 38 B2 32 F8 38
SHA-1 Fingerprint: 23 2A 9E 45 ED 01 68 1C 4E 18 3E CD F3 5E 7F C5 CD 2E 50 BA
MD5 Fingerprint: 20 A8 69 C2 E3 D8 0B 38 6B B5 9E 65 05 DA 95 FC


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV6gAwIBAgIQT18bYB+d7bp8fO/
B9CoP5zAKBggqhkjOPQQDAjAzMTEwLwYDVQQDEyhDYWRkeSBMb2NhbCBBdXRob3JpdHkgLSBFQ0MgSW50ZXJtZWRpYXRlMB4XDTI0MDYyNjA2MzgxM
 [...]
```

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: 4F 5F 1B 60 1F 9D ED BA 7C 7C EF C1 F4 2A 0F E7

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:38:10 2024 GMT
Not Valid After: Jun 26 18:38:10 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 06 56 D3 96 CE 6B 21 8A CF C8 40 95 C8 78 66 4A 29 8C 3F 8D
              D1 39 1F E1 9D CE 1C 2E 60 C6 77 6F
Public Key Y: 58 D6 1B D8 5F 07 5B CF A0 D9 04 9B 7C E0 93 38 E0 D5 12 C4
```

```
              EB 33 0F E6 AC CF 29 8C 3F 06 C2 51

Signature Length: 72 bytes / 576 bits
Signature: 00 30 46 02 21 00 B8 65 36 08 5A 0B DE 52 B1 92 C0 ED 83 59
           94 7B 29 18 D2 11 5F 8F A1 1A CA 7C 63 32 84 D1 FD 1B 02 21
           00 A2 7C 16 3C 8F 32 FD 7C 48 F4 D5 14 36 10 0B AB 30 06 FA
           2C C2 72 3D 4E 33 D6 64 01 88 C5 41 BD

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: 06 85 F0 00 D4 F1 9A 13 96 13 9F A6 E3 6D 9F 5A 97 66 E6 1D


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: FB 63 D0 CB 34 45 D8 8A C0 57 3A 13 79 75 51 7A B4 DB 95 DB


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV6gAwIBAgIQT18bYB+d7bp8fO/
B9CoP5zAKBggqhkjOPQQDAjAzMTEwLwYDVQQDEyhDYWRkeSBMb2NhbCBBdXRob3JpdHkgLSBFQ0MgSW50ZXJtZWRpYXRlMB4XDTI0MDYyNjA2MzgxM
+N0Tkf4Z3OHC5gxndvWNYb2F8HW8+g2QSbfOCTOODVEsTrMw/mrM8pjD8GwlGjgYYwgYMwDgYDVR0PAQH/
BAQDAgeAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUBoXwANTxmhOWE5+m422fWpdm5h0wHwYDVR0jBBgwFoAU
+2PQyzRF2IrAVzoTeXVRerTbldswEgYDVR0RAQH/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: 4F 5F 1B 60 1F 9D ED BA 7C 7C EF C1 F4 2A 0F E7

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:38:10 2024 GMT
Not Valid After: Jun 26 18:38:10 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 06 56 D3 96 CE 6B 21 8A CF C8 40 95 C8 78 66 4A 29 8C 3F 8D
              D1 39 1F E1 9D CE 1C 2E 60 C6 77 6F
Public Key Y: 58 D6 1B D8 5F 07 5B CF A0 D9 04 9B 7C E0 93 38 E0 D5 12 C4
```

```
              EB 33 0F E6 AC CF 29 8C 3F 06 C2 51

Signature Length: 72 bytes / 576 bits
Signature: 00 30 46 02 21 00 B8 65 36 08 5A 0B DE 52 B1 92 C0 ED 83 59
           94 7B 29 18 D2 11 5F 8F A1 1A CA 7C 63 32 84 D1 FD 1B 02 21
           00 A2 7C 16 3C 8F 32 FD 7C 48 F4 D5 14 36 10 0B AB 30 06 FA
           2C C2 72 3D 4E 33 D6 64 01 88 C5 41 BD

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: 06 85 F0 00 D4 F1 9A 13 96 13 9F A6 E3 6D 9F 5A 97 66 E6 1D


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: FB 63 D0 CB 34 45 D8 8A C0 57 3A 13 79 75 51 7A B4 DB 95 DB


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :
```

```
-----BEGIN CERTIFICATE-----
MIIBuTCCAV6gAwIBAgIQT18bYB+d7bp8fO/
B9CoP5zAKBggqhkjOPQQDAjAzMTEwLwYDVQQDEyhDYWRkeSBMb2NhbCBBdXRob3JpdHkgLSBFQ0MgSW50ZXJtZWRpYXRlMB4XDTI0MDYyNjA2MzgxM
+N0Tkf4Z3OHC5gxndvWNYb2F8HW8+g2QSbfOCTOODVEsTrMw/mrM8pjD8GwlGjgYYwgYMwDgYDVR0PAQH/
BAQDAgeAMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAdBgNVHQ4EFgQUBoXwANTxmhOWE5+m422fWpdm5h0wHwYDVR0jBBgwFoAU
+2PQyzRF2IrAVzoTeXVRerTbldswEgYDVR0RAQH/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/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  1.1.1  amd64  The installer of the Anapaya appliance.
  ii   anapaya-system-config  1.0.0  amd64  System configuration for Anapaya appliances.
  ii   apparmor  3.0.4-2ubuntu2.2  amd64  user-space parser utility for AppArmor
  ii   apport  2.20.11-0ubuntu82.5  all  automatically generate crash reports for debugging
  ii   apport-symptoms  0.24  all  symptom scripts for apport
  ii   apt  2.4.9  amd64  commandline package manager
  ii   apt-transport-https  2.4.10  all  transitional package for https support
  ii   apt-utils  2.4.9  amd64  package management related utility programs
  ii   base-files  12ubuntu4.4  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  amd64  GNU Bourne Again SHell
  ii   bash-completion  1:2.11-5ubuntu1  all  programmable completion for the bash shell
  ii   bc  1.07.1-3build1  amd64  GNU bc arbitrary precision calculator language
  ii   bcache-tools  1.0.8-4ubuntu3  amd64  bcache userspace tools
  ii   bind9-dnsutils  1:9.18.12-0ubuntu0.22.04.3  amd64  Clients provided with BIND 9
  ii   bind9-host  1:9.18.12-0ubuntu0.22.04.3  amd64  DNS Lookup Utility
  ii   bind9-libs  1:9.18.12-0ubuntu0.22.04.3  amd64  Shared Libraries used by BIND 9
  ii   binutils  2.38-4ubuntu2.3  amd64  GNU assembler, linker and binary utilities
```

```
 ii   binutils-common  2.38-4ubuntu2.3  amd64  Common files for the GNU assembler, linker and
binary utilities
 ii   binutils-x86-64-linux-gnu  2.38-4ubuntu2.3  amd64  GNU binary utilities, for x86-64-linux-gnu
target
 ii   bolt  0.9.2-1  amd64  system daemon to manage thunderbolt 3 devices
 ii   bsdextrautils  2.37.2-4ubuntu3  amd64  extra utilities from 4.4BSD-Lite
 ii   bsdutils  [...]
```

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: 2024/06/24

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: 2024/04/24

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
```

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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 11 installs of XZ Utils:

  Path    : /var/lib/docker/
overlay2/6a0181bf6433cb0787f1211675e09ad050f9d88595a5324e8d6d401cb8cbaee2/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version : 5.2.5
  Path    : /var/lib/docker/
overlay2/598a8b880b81764a79487c874ee7cab3a394bbb3c6560b38d9cc43d31d146240/diff/usr/lib/
liblzma.so.5.2.9
  Version : 5.2.9

  Path    : /var/lib/docker/overlay2/
d0ce4ed43637013d460acbb5966595c423829375169e9719ee915b6bf58aff93/merged/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version : 5.2.5

  Path    : /snap/snapd/20290/lib/x86_64-linux-gnu/liblzma.so.5.0.0
  Version : 5.0.0

  Path               : /usr/bin/xz
  Version            : 5.2.5
  Associated Package : xz-utils 5.2.5-2ubuntu1
  Managed by OS      : True

  Path    : /snap/lxd/24322/bin/xz
  Version : 5.2.4

  Path    : /snap/snapd/19457/lib/x86_64-linux-gnu/liblzma.so.5.0.0
  Version : 5.0.0

  Path    : /var/lib/docker/
overlay2/0c76b5b0d25455f0eb98841db9773ada467e7a3a51b207d49814636f4d191bf3/merged/bin/xz
  Version : unknown

  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
  Managed by OS      : True

  Path    : /snap/core20/1974/usr/lib/x86_64-linux-gnu/liblzma.so.5.2.4
  Version : 5.2.4
```

191054 - Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : OpenSSL update (USN-6663-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 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-6663-1 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-6663-1

Solution

Update the affected packages.

Risk Factor

None

References

XREF	USN:6663-1

Plugin Information

Published: 2024/02/27, Modified: 2024/02/27

Plugin Output

tcp/0

```
  - Installed package : libssl3_3.0.2-0ubuntu1.10
  - Fixed package     : libssl3_3.0.2-0ubuntu1.15

  - Installed package : openssl_3.0.2-0ubuntu1.10
  - Fixed package     : openssl_3.0.2-0ubuntu1.15
```

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
```

187919 - Ubuntu 22.04 LTS : GNU C Library regression (USN-6541-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6541-2 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-6541-2

Solution

Update the affected packages.

Risk Factor

None

References

XREF	USN:6541-2

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.4
  - Fixed package     : libc-bin_2.35-0ubuntu3.6

  - Installed package : libc6_2.35-0ubuntu3.4
  - Fixed package     : libc6_2.35-0ubuntu3.6

  - Installed package : locales_2.35-0ubuntu3.4
  - Fixed package     : locales_2.35-0ubuntu3.6
```

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: 2024/05/31

Plugin Output

tcp/0

```
This machine is attached to an Ubuntu Pro subscription.

Binary Path                   : /var/lib/ubuntu-advantage
Binary Version                : 28.1~22.04

Enabled Ubuntu Pro Services   :
```

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 167988 13800 ?        Ss     2023 769:20 /sbin/init noquiet nosplash nofb
root           2  0.0  0.0      0     0 ?        S      2023   0:06 [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  13:59 [ksoftirqd/0]
root          14  0.0  0.0      0     0 ?        I      2023 241:52 [rcu_sched]
root          15  0.0  0.0      0     0 ?        S      2023   0:45 [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   0:58 [migration/1]
root          22  0.0  0.0      0     0 ?        S      2023   3:08 [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   0:18 [migration/2]
root          28  0.0  0.0      0     0 ?        S      2023   0:03 [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 06 04 00 00 00 00 00 00 05 00 00 40 00       .............@.


Nessus detected the following process listening on this port :

/app/scion-all
```

186361 - VMWare Tools or Open VM Tools Installed (Linux)

Synopsis

VMWare Tools or Open VM Tools were detected on the remote Linux host.

Description

VMWare Tools or Open VM Tools were detected on the remote Linux host.

See Also

https://kb.vmware.com/s/article/340

http://www.nessus.org/u?c0628155

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/11/28, Modified: 2024/06/24

Plugin Output

tcp/0

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

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: 2024/06/24

Plugin Output

tcp/0

```

Nessus detected 4 installs of Vim:

  Path    : /usr/bin/vim.tiny
  Version : 8.2

  Path    : /usr/bin/vim.basic
  Version : 8.2

  Path    : /snap/lxd/24322/bin/vim.tiny
  Version : 8.1

  Path    : /snap/core20/1974/usr/bin/vim.tiny
  Version : 8.1
```

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.5fc880d2a2e21be0.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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 3 installs of libcurl:

  Path               : /usr/lib/x86_64-linux-gnu/libcurl.so.4.7.0
  Version            : 7.81.0
  Associated Package : libcurl4 7.81.0-1ubuntu1.14
  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 7.81.0-1ubuntu1.14
  Managed by OS      : True
```

```
    Path    : /snap/lxd/24322/lib/x86_64-linux-gnu/libcurl-gnutls.so.4.6.0
    Version : 7.68.0
```

192.168.111.1

128	121	199	1	109
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jun 26 10:47:32 2024
End time:	Wed Jun 26 11:10:49 2024

Host Information

IP:	192.168.111.1
MAC Address:	02:42:E4:E0:1C:30 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 5.15.0-86-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

7.7

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1l
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1l
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
```

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

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

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

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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
```

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/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/
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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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
```

194474 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1)

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 / 24.04 LTS. host has a package installed that is affected by a vulnerability as referenced in the USN-6756-1 advisory.

- less through 653 allows OS command execution via a newline character in the name of a file, because quoting is mishandled in filename.c. Exploitation typically requires use with attacker-controlled file names, such as the files extracted from an untrusted archive. Exploitation also requires the LESSOPEN environment variable, but this is set by default in many common cases. (CVE-2024-32487)

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-6756-1

Solution

Update the affected less package.

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

7.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-32487
XREF	USN:6756-1

Plugin Information

Published: 2024/04/29, Modified: 2024/04/29

Plugin Output

tcp/0

```
  - Installed package : less_590-1ubuntu0.22.04.2
  - Fixed package     : less_590-1ubuntu0.22.04.3
```

193362 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1)

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-6736-1 advisory.

- inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9840)

- inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9841)

- zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. (CVE-2018-25032)

- zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference). (CVE-2022-37434)

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-6736-1

Solution

Update the affected klibc-utils, libklibc and / or libklibc-dev 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

6.7

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

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

References

CVE	CVE-2016-9840
CVE	CVE-2016-9841
CVE	CVE-2018-25032
CVE	CVE-2022-37434
XREF	USN:6736-1

Plugin Information

Published: 2024/04/16, Modified: 2024/04/16

Plugin Output

tcp/0

```
  - Installed package : klibc-utils_2.0.10-4
  - Fixed package     : klibc-utils_2.0.10-4ubuntu0.1

  - Installed package : libklibc_2.0.10-4
  - Fixed package     : libklibc_2.0.10-4ubuntu0.1
```

193515 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU C Library vulnerability (USN-6737-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6737-1 advisory.

- The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable. (CVE-2024-2961)

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-6737-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-2961
XREF	USN:6737-1

Plugin Information

Published: 2024/04/18, Modified: 2024/04/19

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.6
  - Fixed package     : libc-bin_2.35-0ubuntu3.7

  - Installed package : libc6_2.35-0ubuntu3.6
  - Fixed package     : libc6_2.35-0ubuntu3.7

  - Installed package : locales_2.35-0ubuntu3.6
  - Fixed package     : locales_2.35-0ubuntu3.7
```

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

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 5.15.0-86-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

6.7

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 5.15.0-86-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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

6.7

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

6.7

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/
overlay2/5158c6493f95050aa5912736f623184aa523fc0de0df8f42e543ca14650234c6/diff/lib/libcrypto.so.3
  Reported version : 3.0.10
  Fixed version    : 3.0.11
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

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/
overlay2/5158c6493f95050aa5912736f623184aa523fc0de0df8f42e543ca14650234c6/diff/lib/libcrypto.so.3
  Reported version : 3.0.10
  Fixed version    : 3.0.12
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

3.6

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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
```

192219 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1)

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-6698-1 advisory.

- Vim before 9.0.2142 has a stack-based buffer overflow because did_set_langmap in map.c calls sprintf to write to the error buffer that is passed down to the option callback functions. (CVE-2024-22667)

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-6698-1

Solution

Update the affected packages.

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

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-2024-22667
XREF	USN:6698-1

Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

Plugin Output

tcp/0

```

  - Installed package : vim_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-common_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim-common_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-runtime_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim-runtime_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-tiny_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim-tiny_2:8.2.3995-1ubuntu2.16

  - Installed package : xxd_2:8.2.3995-1ubuntu2.15
  - Fixed package     : xxd_2:8.2.3995-1ubuntu2.16

```

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

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
```

198244 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6804-1 advisory.

It was discovered that GNU C Library nscd daemon contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33599)

It was discovered that GNU C Library nscd daemon did not properly check the cache content, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33600)

It was discovered that GNU C Library nscd daemon did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33601)

It was discovered that GNU C Library nscd daemon did not properly handle memory allocation, which could lead to memory corruption. A local attacker could use this to cause a denial of service (system crash).
(CVE-2024-33602)

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-6804-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-33599
CVE	CVE-2024-33600
CVE	CVE-2024-33601
CVE	CVE-2024-33602
XREF	USN:6804-1

Plugin Information

Published: 2024/05/31, Modified: 2024/05/31

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.6
  - Fixed package     : libc-bin_2.35-0ubuntu3.8

  - Installed package : libc6_2.35-0ubuntu3.6
  - Fixed package     : libc6_2.35-0ubuntu3.8

  - Installed package : locales_2.35-0ubuntu3.6
  - Fixed package     : locales_2.35-0ubuntu3.8
```

198069 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Intel Microcode vulnerabilities (USN-6797-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6797-1 advisory.

It was discovered that some 3rd and 4th Generation Intel Xeon Processors did not properly restrict access to certain hardware features when using Intel SGX or Intel TDX. This may allow a privileged local user to potentially further escalate their privileges on the system. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-22655)

It was discovered that some Intel Atom Processors did not properly clear register state when performing various operations. A local attacker could use this to obtain sensitive information via a transient execution attack. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-28746)

It was discovered that some Intel Processors did not properly clear the state of various hardware structures when switching execution contexts. A local attacker could use this to access privileged information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-38575)

It was discovered that some Intel Processors did not properly enforce bus lock regulator protections. A remote attacker could use this to cause a denial of service. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-39368)

It was discovered that some Intel Xeon D Processors did not properly calculate the SGX base key when using Intel SGX. A privileged local attacker could use this to obtain sensitive information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS.

(CVE-2023-43490)

It was discovered that some Intel Processors did not properly protect against concurrent accesses. A local attacker could use this to obtain sensitive information. (CVE-2023-45733)

It was discovered that some Intel Processors TDX module software did not properly validate input. A privileged local attacker could use this information to potentially further escalate their privileges on the system. (CVE-2023-45745, CVE-2023-47855)

It was discovered that some Intel Core Ultra processors did not properly handle particular instruction sequences. A local attacker could use this issue to cause a denial of service.

(CVE-2023-46103)

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-6797-1

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22655
CVE	CVE-2023-28746
CVE	CVE-2023-38575
CVE	CVE-2023-39368
CVE	CVE-2023-43490
CVE	CVE-2023-45733
CVE	CVE-2023-45745
CVE	CVE-2023-46103
CVE	CVE-2023-47855
XREF	USN:6797-1

Plugin Information

Published: 2024/05/29, Modified: 2024/05/29

Plugin Output

tcp/0

```
  - Installed package : intel-microcode_3.20231114.0ubuntu0.22.04.1
  - Fixed package     : intel-microcode_3.20240514.0ubuntu0.22.04.1
```

193905 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1)

Synopsis

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

Description

The remote Ubuntu 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-6754-1 advisory.

- Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both. (CVE-2019-9511)

- Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service.

The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU. (CVE-2019-9513)

- The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. (CVE-2023-44487)

- nghttp2 is an implementation of the Hypertext Transfer Protocol version 2 in C. The nghttp2 library prior to version 1.61.0 keeps reading the unbounded number of HTTP/2 CONTINUATION frames even after a stream is reset to keep HPACK context in sync. This causes excessive CPU usage to decode HPACK stream. nghttp2 v1.61.0 mitigates this vulnerability by limiting the number of CONTINUATION frames it accepts per stream.

There is no workaround for this vulnerability. (CVE-2024-28182)

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-6754-1

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

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

VPR Score

6.1

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

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

References

CVE	CVE-2019-9511
CVE	CVE-2019-9513
CVE	CVE-2023-44487
CVE	CVE-2024-28182
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	USN:6754-1
XREF	CEA-ID:CEA-2024-0004
XREF	CEA-ID:CEA-2019-0643

Plugin Information

Published: 2024/04/25, Modified: 2024/04/26

Plugin Output

tcp/0

```
  - Installed package : libnghttp2-14_1.43.0-1ubuntu0.1
  - Fixed package     : libnghttp2-14_1.43.0-1ubuntu0.2
```

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

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 : libglib2.0-0_2.72.4-0ubuntu2.2
  - Fixed package     : libglib2.0-0_2.72.4-0ubuntu2.3

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

192621 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1)

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-6718-1 advisory.

- When a protocol selection parameter option disables all protocols without adding any then the default set of protocols would remain in the allowed set due to an error in the logic for removing protocols. The below command would perform a request to curl.se with a plaintext protocol which has been explicitly disabled. curl --proto -all,-http http://curl.se The flaw is only present if the set of selected protocols disables the entire set of available protocols, in itself a command with no practical use and therefore unlikely to be encountered in real situations. The curl security team has thus assessed this to be low severity bug. (CVE-2024-2004)

- 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.

(CVE-2024-2398)

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-6718-1

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

4.4

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-2024-2004
CVE	CVE-2024-2398
XREF	USN:6718-1
XREF	IAVA:2024-A-0185

Plugin Information

Published: 2024/03/27, Modified: 2024/03/29

Plugin Output

tcp/0

```
  - Installed package : curl_7.81.0-1ubuntu1.15
  - Fixed package     : curl_7.81.0-1ubuntu1.16

  - Installed package : libcurl3-gnutls_7.81.0-1ubuntu1.15
  - Fixed package     : libcurl3-gnutls_7.81.0-1ubuntu1.16

  - Installed package : libcurl4_7.81.0-1ubuntu1.15
  - Fixed package     : libcurl4_7.81.0-1ubuntu1.16
```

191019 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : libxml2 vulnerability (USN-6658-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6658-1 advisory.

- An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free. (CVE-2024-25062)

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-6658-1

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

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

VPR Score

4.4

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

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

STIG Severity

II

References

CVE	CVE-2024-25062
XREF	IAVA:2024-A-0067
XREF	USN:6658-1

Plugin Information

Published: 2024/02/26, Modified: 2024/03/11

Plugin Output

tcp/0

```
  - Installed package : libxml2_2.9.13+dfsg-1ubuntu0.3
  - Fixed package     : libxml2_2.9.13+dfsg-1ubuntu0.4
```

192629 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-1 advisory.

- wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover. (CVE-2024-28085)

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-6719-1

Solution

Update the affected packages.

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

7.9

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

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

References

CVE	CVE-2024-28085
XREF	USN:6719-1

Plugin Information

Published: 2024/03/27, Modified: 2024/03/29

Plugin Output

tcp/0

```
  - Installed package : bsdextrautils_2.37.2-4ubuntu3
  - Fixed package     : bsdextrautils_2.37.2-4ubuntu3.3

  - Installed package : bsdutils_1:2.37.2-4ubuntu3
  - Fixed package     : bsdutils_1:2.37.2-4ubuntu3.3

  - Installed package : eject_2.37.2-4ubuntu3
  - Fixed package     : eject_2.37.2-4ubuntu3.3

  - Installed package : fdisk_2.37.2-4ubuntu3
  - Fixed package     : fdisk_2.37.2-4ubuntu3.3

  - Installed package : libblkid1_2.37.2-4ubuntu3
  - Fixed package     : libblkid1_2.37.2-4ubuntu3.3

  - Installed package : libfdisk1_2.37.2-4ubuntu3
  - Fixed package     : libfdisk1_2.37.2-4ubuntu3.3

  - Installed package : libmount1_2.37.2-4ubuntu3
  - Fixed package     : libmount1_2.37.2-4ubuntu3.3

  - Installed package : libsmartcols1_2.37.2-4ubuntu3
  - Fixed package     : libsmartcols1_2.37.2-4ubuntu3.3

  - Installed package : libuuid1_2.37.2-4ubuntu3
  - Fixed package     : libuuid1_2.37.2-4ubuntu3.3

  - Installed package : mount_2.37.2-4ubuntu3
  - Fixed package     : mount_2.37.2-4ubuntu3.3

  - Installed package : util-linux_2.37.2-4ubuntu3
  - Fixed package     : util-linux_2.37.2-4ubuntu3.3
```

193159 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-2 advisory.

- wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover. (CVE-2024-28085)

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-6719-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28085
XREF	USN:6719-2

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : bsdextrautils_2.37.2-4ubuntu3
  - Fixed package     : bsdextrautils_2.37.2-4ubuntu3.4

  - Installed package : bsdutils_1:2.37.2-4ubuntu3
  - Fixed package     : bsdutils_1:2.37.2-4ubuntu3.4

  - Installed package : eject_2.37.2-4ubuntu3
  - Fixed package     : eject_2.37.2-4ubuntu3.4

  - Installed package : fdisk_2.37.2-4ubuntu3
  - Fixed package     : fdisk_2.37.2-4ubuntu3.4

  - Installed package : libblkid1_2.37.2-4ubuntu3
  - Fixed package     : libblkid1_2.37.2-4ubuntu3.4

  - Installed package : libfdisk1_2.37.2-4ubuntu3
  - Fixed package     : libfdisk1_2.37.2-4ubuntu3.4

  - Installed package : libmount1_2.37.2-4ubuntu3
  - Fixed package     : libmount1_2.37.2-4ubuntu3.4

  - Installed package : libsmartcols1_2.37.2-4ubuntu3
  - Fixed package     : libsmartcols1_2.37.2-4ubuntu3.4

  - Installed package : libuuid1_2.37.2-4ubuntu3
  - Fixed package     : libuuid1_2.37.2-4ubuntu3.4

  - Installed package : mount_2.37.2-4ubuntu3
  - Fixed package     : mount_2.37.2-4ubuntu3.4

  - Installed package : util-linux_2.37.2-4ubuntu3
  - Fixed package     : util-linux_2.37.2-4ubuntu3.4
```

183454 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6446-1)

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-6446-1 advisory.

- The fix for XSA-423 added logic to Linux'es netback driver to deal with a frontend splitting a packet in a way such that not all of the headers would come in one piece. Unfortunately the logic introduced there didn't account for the extreme case of the entire packet being split into as many pieces as permitted by the protocol, yet still being smaller than the area that's specially dealt with to keep all (possible) headers together. Such an unusual packet would therefore trigger a buffer overrun in the driver.

(CVE-2023-34319)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Due to a race condition between nf_tables netlink control plane transaction and nft_set element garbage collection, it is possible to underflow the reference counter causing a use-after-free vulnerability. We recommend upgrading past commit 3e91b0ebd994635df2346353322ac51ce84ce6d8. (CVE-2023-4244)

- An integer overflow flaw was found in the Linux kernel. This issue leads to the kernel allocating `skb_shared_info` in the userspace, which is exploitable in systems without SMAP protection since `skb_shared_info` contains references to function pointers. (CVE-2023-42752)

- An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could lead to a miscalculation of the `h->nets` array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system. (CVE-2023-42753)

- A flaw was found in the IPv4 Resource Reservation Protocol (RSVP) classifier in the Linux kernel. The xprt pointer may go beyond the linear part of the skb, leading to an out-of-bounds read in the `rsvp_classify` function. This issue may allow a local user to crash the system and cause a denial of service.

(CVE-2023-42755)

- A flaw was found in the Netfilter subsystem of the Linux kernel. A race condition between IPSET_CMD_ADD and IPSET_CMD_SWAP can lead to a kernel panic due to the invocation of `__ip_set_put` on a wrong `set`.

This issue may allow a local user to crash the system. (CVE-2023-42756)

- A use-after-free vulnerability in the Linux kernel's af_unix component can be exploited to achieve local privilege escalation. The unix_stream_sendpage() function tries to add data to the last skb in the peer's recv queue without locking the queue. Thus there is a race where unix_stream_sendpage() could access an skb locklessly that is being released by garbage collection, resulting in use-after-free. We recommend upgrading past commit 790c2f9d15b594350ae9bca7b236f2b1859de02c. (CVE-2023-4622)

- A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploited to achieve local privilege escalation. If a class with a link-sharing curve (i.e. with the HFSC_FSC flag set) has a parent without a link-sharing curve, then init_vf() will call vttree_insert() on the parent, but vttree_remove() will be skipped in update_vf(). This leaves a dangling pointer that can cause a use-after-free. We recommend upgrading past commit b3d26c5702c7d6c45456326e56d2ccf3f103e60f. (CVE-2023-4623)

- Rejected reason: CVE-2023-4881 was wrongly assigned to a bug that was deemed to be a non-security issue by the Linux kernel security team. (CVE-2023-4881)

- A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. When the plug qdisc is used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect .peek handler of sch_plug and lack of error checking in agg_dequeue(). We recommend upgrading past commit 8fc134fee27f2263988ae38920bc03da416b03d8. (CVE-2023-4921)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Addition and removal of rules from chain bindings within the same transaction causes leads to use-after-free. We recommend upgrading past commit f15f29fd4779be8a418b66e9d52979bb6d6c2325. (CVE-2023-5197)

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-6446-1

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

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-2023-4244
CVE	CVE-2023-4622
CVE	CVE-2023-4623
CVE	CVE-2023-4881
CVE	CVE-2023-4921
CVE	CVE-2023-5197
CVE	CVE-2023-34319
CVE	CVE-2023-42752
CVE	CVE-2023-42753
CVE	CVE-2023-42755
CVE	CVE-2023-42756
XREF	USN:6446-1

Plugin Information

Published: 2023/10/20, Modified: 2024/01/09

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-86-generic does not meet the minimum fixed level of 5.15.0-87-generic
 for this advisory.
```

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

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 5.15.0-86-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

8.4

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 5.15.0-86-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

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 5.15.0-86-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

6.7

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 5.15.0-86-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

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 5.15.0-86-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

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 5.15.0-86-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

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 5.15.0-86-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

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 5.15.0-86-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

6.7

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 5.15.0-86-generic does not meet the minimum fixed level of 5.15.0-112-
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

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
```

200099 - Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : libarchive vulnerability (USN-6805-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6805-1 advisory.

It was discovered that libarchive incorrectly handled certain RAR archive files. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

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-6805-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-26256
XREF	USN:6805-1

Plugin Information

Published: 2024/06/04, Modified: 2024/06/04

Plugin Output

tcp/0

```
  - Installed package : libarchive13_3.6.0-1ubuntu1
  - Fixed package     : libarchive13_3.6.0-1ubuntu1.1
```

192198 - Ubuntu 22.04 LTS : Bash vulnerability (USN-6697-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6697-1 advisory.

- A flaw was found in the bash package, where a heap-buffer overflow can occur in valid parameter_transform.

This issue may lead to memory problems. (CVE-2022-3715)

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-6697-1

Solution

Update the affected bash, bash-builtins and / or bash-static packages.

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

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-2022-3715
XREF	USN:6697-1

Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

Plugin Output

tcp/0

```
  - Installed package : bash_5.1-6ubuntu1
  - Fixed package     : bash_5.1-6ubuntu1.1
```

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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version     : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

2.9

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
```

```
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/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/
a61d71551040a2dbcdc9486754d5893a95daa05630eb3fe595ebaff12f2fedd1/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

5.9

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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/merged/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/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/
a61d71551040a2dbcdc9486754d5893a95daa05630eb3fe595ebaff12f2fedd1/diff/usr/bin/openssl
  Reported version : 1.1.1w
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/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

2.9

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

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/
overlay2/5158c6493f95050aa5912736f623184aa523fc0de0df8f42e543ca14650234c6/diff/lib/libcrypto.so.3
  Reported version : 3.0.10
  Fixed version    : 3.0.13
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

5.9

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/
overlay2/5158c6493f95050aa5912736f623184aa523fc0de0df8f42e543ca14650234c6/diff/lib/libcrypto.so.3
  Reported version : 3.0.10
  Fixed version    : 3.0.14
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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

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/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/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/
d30a91b2a27649c19ddedcd55b280b1dc7d55f4eb76a0355dc125ba7f0138ab0/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
```

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
```

198044 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2 vulnerability (USN-6787-1)

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 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6787-1 advisory.

It was discovered that Jinja2 incorrectly handled certain HTML attributes that were accepted by the xmlattr filter. An attacker could use this issue to inject arbitrary HTML attribute keys and values to potentially execute a cross-site scripting (XSS) attack.

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-6787-1

Solution

Update the affected python-jinja2 and / or python3-jinja2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.3

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

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

References

CVE	CVE-2024-34064
XREF	USN:6787-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : python3-jinja2_3.0.3-1ubuntu0.1
  - Fixed package     : python3-jinja2_3.0.3-1ubuntu0.2
```

200307 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1)

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 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6827-1 advisory.

It was discovered that LibTIFF incorrectly handled memory when

performing certain cropping operations, leading to a heap buffer overflow. An attacker could use this issue to cause a

denial of service, or possibly execute arbitrary code.

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-6827-1

Solution

Update the affected packages.

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

3.6

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-2023-3164
XREF	USN:6827-1

Plugin Information

Published: 2024/06/11, Modified: 2024/06/11

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6ubuntu0.8
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.9
```

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

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

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.
```

197569 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 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-6780-1 advisory.

Guido Vranken discovered that idna did not properly manage certain inputs,

which could lead to significant resource consumption. 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-6780-1

Solution

Update the affected pypy-idna, python-idna and / or python3-idna 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:N/I:N/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-3651
XREF	USN:6780-1

Plugin Information

Published: 2024/05/21, Modified: 2024/05/23

Plugin Output

tcp/0

```

  - Installed package : python3-idna_3.3-1
  - Fixed package     : python3-idna_3.3-1ubuntu0.1

```

198063 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : TPM2 Software Stack vulnerabilities (USN-6796-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6796-1 advisory.

Fergus Dall discovered that TPM2 Software Stack did not properly handle layer arrays. An attacker could possibly use this issue to cause

TPM2 Software Stack to crash, resulting in a denial of service, or

possibly execute arbitrary code. (CVE-2023-22745)

Jurgen Repp and Andreas Fuchs discovered that TPM2 Software Stack did not

validate the quote data after deserialization. An attacker could generate an arbitrary quote and cause TPM2 Software Stack to have unknown behavior.

(CVE-2024-29040)

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-6796-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

5.9 (CVSS2#AV:L/AC:H/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22745
CVE	CVE-2024-29040
XREF	USN:6796-1

Plugin Information

Published: 2024/05/29, Modified: 2024/05/29

Plugin Output

tcp/0

```
  - Installed package : libtss2-esys-3.0.2-0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-esys-3.0.2-0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-mu0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-mu0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-sys1_3.2.0-1ubuntu1
  - Fixed package     : libtss2-sys1_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-cmd0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-cmd0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-device0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-device0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-mssim0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-mssim0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-swtpm0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-swtpm0_3.2.0-1ubuntu1.1
```

194475 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU cpio vulnerabilities (USN-6755-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6755-1 advisory.

- Debian's cpio contains a path traversal vulnerability. This issue was introduced by reverting CVE-2015-1197 patches which had caused a regression in --no-absolute-filenames. Upstream has since provided a proper fix to --no-absolute-filenames. (CVE-2023-7207)

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-6755-1

Solution

Update the affected cpio and / or cpio-win32 packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-7207
XREF	USN:6755-1

Plugin Information

Published: 2024/04/29, Modified: 2024/04/29

Plugin Output

tcp/0

```
  - Installed package : cpio_2.13+dfsg-7
  - Fixed package     : cpio_2.13+dfsg-7ubuntu0.1
```

193341 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GnuTLS vulnerabilities (USN-6733-1)

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-6733-1 advisory.

- A flaw was found in GnuTLS. The Minerva attack is a cryptographic vulnerability that exploits deterministic behavior in systems like GnuTLS, leading to side-channel leaks. In specific scenarios, such as when using the GNUTLS_PRIVKEY_FLAG_REPRODUCIBLE flag, it can result in a noticeable step in nonce size from 513 to 512 bits, exposing a potential timing side-channel. (CVE-2024-28834)

- A flaw has been discovered in GnuTLS where an application crash can be induced when attempting to verify a specially crafted .pem bundle using the certtool --verify-chain command. (CVE-2024-28835)

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-6733-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28834
CVE	CVE-2024-28835
XREF	USN:6733-1

Plugin Information

Published: 2024/04/15, Modified: 2024/04/15

Plugin Output

tcp/0

```
  - Installed package : libgnutls30_3.7.3-4ubuntu1.4
  - Fixed package     : libgnutls30_3.7.3-4ubuntu1.5
```

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

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 5.15.0-86-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

6.7

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 5.15.0-86-generic does not meet the minimum fixed level of 5.15.0-107-
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

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 difference between the local and remote clocks is -2 seconds.
```

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: 2024/06/24

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: 2024/06/24

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:25.0.3 -> 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:3.0.10 -> OpenSSL Project OpenSSL
  cpe:/a:openssl:openssl:3.0.2 -> 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:5.2.9 -> 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: 2024/06/24

Plugin Output

tcp/0

```
Path               : /usr/bin/curl
Version            : 7.81.0
Associated Package : curl 7.81.0-1ubuntu1.15
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: 2024-06-26 08:49:00
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: 2024/06/24

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: 2024/06/24

Plugin Output

tcp/0

```
Docker container dea9d413aa4e6c81cc50bc0a2abf83136224ba98f3c7b340aa3d582d1c726a49 has 7 changed
 files

Docker container 467c702d266a24f7161dde71be5bd7ac23fcd74f757f308f99da46c9b50f9601 has 18 changed
 files

Docker container 59307a95ce1ad9c488f6e3251d1ea27dc4899fcaecac3fff7da743889de3d7a4 has 26 changed
 files

Docker container 55c0c98a006f9fbc64dd01749f51cfb4bc953ee4292ccd480145ac7fd8def28f has 6 changed
 files

Docker container aecec6366a92cad27e3a0575c38855dbf3d5b6a27c6e816ec4197eca0afa08f6 has 6 changed
 files

Docker container 9e9bcdda183bdb00d257d0406ae9d6709c281e3b9efff8aa66209643a44311ce has 14 changed
 files

Docker container 1d776cbdd0d463dd04f1a9d93d43ebc7daab59cbaaa9adc1c362b4f4b853c9fe has 3 changed
 files

Docker container e2cc5042a66ba3dfd375ca872c8c5fcc42a69e6a189937737df0d867bbb3704e has 6 changed
 files
```

```
Docker container 26617ac9f29bc37ef6aab11cd2bd6bca652b084eb3c185c6903e974ae561f1eb has 6 changed
 files

Docker container 66387d931de837fd56c2f7dbba0a620de1474743eb45239a0e3963e8bb78cfac has 5 changed
 files

Docker container 3a339e36fe870fb2de2ca39ca4951443698d7579023a7063769d8af50f60e428 has 9 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: 2024/06/24

Plugin Output

tcp/0

```
  Path    : /usr/bin/docker
  Version : 25.0.3
  build   : 4debf41
```

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: 2024/06/24

Plugin Output

tcp/0

```
    Version: 25.0.3
    Version: 25.0.3
    Version: 1.6.28
    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:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
  Tag:        v0.35.4
  ID:         dea9d413aa4e6c81cc50bc0a2abf83136224ba98f3c7b340aa3d582d1c726a49
  Ports:      n/a

  Name:       /dataplane
  Image:      vpp-dataplane
  Image ID : sha256:2713bb13f7dd53ef4823583e7335fba2f066508afd00380bcff049576934959f
  Tag:        v0.35.4
  ID:         467c702d266a24f7161dde71be5bd7ac23fcd74f757f308f99da46c9b50f9601
  Ports:      n/a

  Name:       /control-64-2_0_2b
  Image:      scion-all
```

```
Image ID : sha256:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
Tag:       v0.35.4
ID:        59307a95ce1ad9c488f6e3251d1ea27dc4899fcaecac3fff7da743889de3d7a4
Ports:     n/a

Name:      /promtail
Image:     promtail
Image ID : sha256:98b1e36a7b1304ae98e571ee63cfba659ff95bb6e579c18694f2979a7f9071e4
Tag:       v0.35.4
ID:        55c0c98a006f9fbc64dd01749f51cfb4bc953ee4292ccd480145ac7fd8def28f
Ports:     n/a

Name:      /router
Image:     scion-all
Image ID : sha256:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
Tag:       v0.35.4
ID:        aecec6366a92cad27e3a0575c38855dbf3d5b6a27c6e816ec4197eca0afa08f6
Ports:     n/a

Name:      /daemon-64-2_0_2b
Image:     scion-all
Image ID : sha256:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
Tag:       v0.35.4
ID:        9e9bcdda183bdb00d257d0406ae9d6709c281e3b9efff8aa66209643a44311ce
Ports:     n/a

Name:      /telemetry
Image:     opentelemetry-collector
Image ID : sha256:bb0d0d8b3897adeafdda039a41065799747ac0e87ce3d36fe1fd058922fe7732
Tag:       v0.35.4
ID:        1d776cbdd0d463dd04f1a9d93d43ebc7daab59cbaaa9adc1c362b4f4b853c9fe
Ports:     n/a

Name:      /dispatcher
Image:     scion-all
Image ID : sha256:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
Tag:       v0.35.4
ID:        e2cc5042a66ba3dfd375ca8 [...]
```

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::1108:b6c6:82f6:6ded (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:e4:e0:1c:30 (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:e4:e0:1c:30
  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::1108:b6c6:82f6:6ded
        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
     - 10.111.8.0/24
     - 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: 2024/06/24

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:E4:E0:1C:30
  - 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: 2021/05/19

Plugin Output

tcp/443/www

```
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
```

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/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: Wed, 26 Jun 2024 08:56:03 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: Wed, 26 Jun 2024 08:56:04 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: Wed, 26 Jun 2024 08:56:03 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: 2024/06/24

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
+ docker0
  + IPv4
    - Address       : 172.17.0.1
      Assign Method : static
+ wg0
  + IPv4
    - Address       : 198.18.30.2
      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::1108:b6c6:82f6:6ded
      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: 2024/06/24

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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 10 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/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/merged/usr/lib/x86_64-
linux-gnu/libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/merged/usr/lib/x86_64-
linux-gnu/libgcrypt.so.20.2.8
  Version : 1.8.8
  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/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   21G  199G  10% /
tmpfs                               32G     0   32G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
overlay                            229G   21G  199G  10% /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged
overlay                            229G   21G  199G  10% /var/lib/docker/
overlay2/45b66544ed5c326970a918cce54381d2f13425ff651d2e2be465e76e32ff195e/merged
overlay                            229G   21G  199G  10% /var/lib/docker/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/merged
overlay                            229G   21G  199G  10% /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged
overlay                            229G   21G  199G  10% /var/lib/docker/overlay2/
ca5e14dcdb98e970431a17929eabe86999ad5fb41af382f37cfda7960016f36f/merged
overlay                            229G   21G  199G  10% /var/lib/docker/
overlay2/1529fb851778cf08d6f6e4831a9ba9e96122f3d12c55cf6af1893bd28c898371/merged
overlay                            229G   21G  199G  10% /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged
overlay                            229G   21G  199G  10% /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged
overlay                            229G   21G  199G  10% /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged
```

```
overlay                           229G   21G  199G  10% /var/lib/docker/overlay2/
da1e654a8b0e930d5adcd862cfe77026211d675977a06068f6cf5b85033f68eb/merged
overlay                           229G   21G  199G  10% /var/lib/docker/overlay2/
bd1f3f2d9ff8f36067000a89303e911e83b888527b9a2b21151f80164225fab5/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: 2024/06/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202406250936
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1404-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 : 63.610 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 : 2024/6/26 10:47 CEST
Scan duration : 1385 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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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 daemon is not managed by dpkg :

/usr/local/bin/appliance
```

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 5.15.0-86-generic on Ubuntu 22.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 5.15.0-86-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 5.15.0-86-generic #96-Ubuntu SMP Wed Sep 20 08:23:49 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 : 27.151217 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: 2024/06/24

Plugin Output

tcp/22/ssh

```
  Service : ssh
  Version : 8.9p1
  Banner  : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6
```

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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 39 installs of OpenSSL:

  Path    : /var/lib/docker/
overlay2/5158c6493f95050aa5912736f623184aa523fc0de0df8f42e543ca14650234c6/diff/lib/libcrypto.so.3
  Version : 3.0.10

  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/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/lib/x86_64-
linux-gnu/libssl.so.1.1
  Version : 1.1.1k
  Path    : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1w

  Path    : /var/lib/docker/overlay2/
c1a011b79be6103aaab6a286d35aac4be730608004f6db3692eca375ba1a6ddd/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/2ed9a3c943fac5562c6fa1d41f5d590b19a1d6b3773fb92105063f997ad7b276/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/
f8756c540a0411885cf5a11306632594f100ab7286720bc2ccc4b1428db88dda/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/6575b20aa0a148e9f62809d0bea7780d9df97bc49445879792ea697e06e04c91/merged/usr/lib/x86_64-
linux-gnu/libcrypto.so.1.1
  Version : 1.1.1k

  Path    : /var/lib/docker/
overlay2/4253c1080877fd8945b83f9c18eeb73206e7a323887853c6bec5f5aa87f8a708/merged/usr/bin/openssl
  Version : 1.1.1k

  Path    : /var/lib/docker/overlay2/bd1f3f2d9ff8f36067000a89303e9 [...]
```

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: 2024/06/11

Plugin Output

tcp/0

```
. You need to take the following 39 actions :

[ OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities (192965) ]

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

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ OpenSSL 3.0.0 < 3.0.14 Multiple Vulnerabilities (192966) ]

+ Action to take : Upgrade to OpenSSL version 3.0.14 or later.

+Impact : Taking this action will resolve 39 different vulnerabilities (CVEs).


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2
 vulnerability (USN-6787-1) (198044) ]

+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 packages.
```

```
[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF
 vulnerability (USN-6827-1) (200307) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less
 vulnerability (USN-6756-1) (194474) ]

+ Action to take : Update the affected less package.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability
 (USN-6698-1) (192219) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities
 (USN-6736-1) (193362) ]

+ Action to take : Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

+Impact : Taking this action will resolve 4 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 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.

+Imp [...]
```

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
```

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

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

Solution

Disable IPv6 if you do not actually using it.

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```

The following global addresss were gathered :

  - ['ipv6': fe80::ae1f:6bff:fe75:11f4]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': fe80::2:0:2b:1]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': fe80::21b:21ff:febe:3452]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': ::1]['scope': host]['scopeid': 0x10]['prefixlen': 128]
  - ['ipv6': fe80::1108:b6c6:82f6:6ded]['scope': link]['scopeid': 0x20]['prefixlen': 64]
```

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: 2023/11/27

Plugin Output

tcp/22/ssh

```
  Process ID   : 506056
  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: 2023/11/27

Plugin Output

udp/30041

```
  Process ID   : 553809
  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: 2023/11/27

Plugin Output

udp/30042

```
  Process ID   : 553814
  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: 2023/11/27

Plugin Output

tcp/30252

```

  Process ID   : 1200785
  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: 2023/11/27

Plugin Output

tcp/42001/www

```
Process ID   : 505313
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: 2024/06/24

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: 2021/01/19

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: 2023/11/27

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: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6
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 : Jun 30 19:38:18 2024 GMT

|-Subject   :
|-Not After : Jun 26 18:37:34 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
Jun 26 18:37:34 2024 GMT :

  Subject          : n/a
  Issuer           : CN=Caddy Local Authority - ECC Intermediate
  Not valid before : Jun 26 06:37:34 2024 GMT
  Not valid after  : Jun 26 18:37:34 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 A4 4E 30 E9 46 DD 50 70 D3 D8 84 6B E3 18 24 A3

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:37:34 2024 GMT
Not Valid After: Jun 26 18:37:34 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 9D DE 08 6C A3 15 CB 7B 12 DC A4 50 6C 8F 08 57 2F 97 03 C6
              82 52 9C ED 9B 4A 67 48 4B DC 94 E2
Public Key Y: 1F 05 E0 44 18 1F 05 EB 08 F2 58 DC 9A E8 C7 DA D6 60 BB 80
              A5 E7 CE 85 53 D5 42 09 13 C2 A7 BA

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 B1 83 C9 90 2D 77 02 CE C4 C9 3D 5A 4E A8
           82 07 2F AF 5D BB C6 21 4B DC 31 35 7B DB 63 17 E8 92 02 20
           3A 73 92 26 60 C4 4D 08 45 A9 C5 99 15 0D B6 0B F5 12 78 AC
           16 F9 B9 57 2E B3 B1 55 AD EE 63 C3
```

```
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: 9C A4 C4 40 35 0F 2D 9C 56 1C 0B 4D 57 FE D7 CA A7 D3 BE BD


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: C5 B3 0E 5E 42 06 77 F1 F7 A8 C7 0B 92 05 F2 BB 07 DD 7F 41


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1


Fingerprints :

SHA-256 Fingerprint: 84 A2 0A DE 71 E4 3D E7 CE B0 F4 C3 49 72 9C B7 A7 F6 98 84
                     85 52 A8 E4 76 A0 51 CE BA 52 F6 1E
SHA-1 Fingerprint: B0 1C 60 5D 9C FC 99 76 21 DD 34 63 43 A7 C6 60 CC 7B 49 C2
MD5 Fingerprint: DC FB 30 43 5D C5 57 95 C2 DB A3 EF 0A 36 7D 8F


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV+gAwIBAgIRAKROMOlG3VBw09iEa
+MYJKMwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA2MjYwNjM3MzF
 [...]
```

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 A4 4E 30 E9 46 DD 50 70 D3 D8 84 6B E3 18 24 A3

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:37:34 2024 GMT
Not Valid After: Jun 26 18:37:34 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 9D DE 08 6C A3 15 CB 7B 12 DC A4 50 6C 8F 08 57 2F 97 03 C6
             82 52 9C ED 9B 4A 67 48 4B DC 94 E2
Public Key Y: 1F 05 E0 44 18 1F 05 EB 08 F2 58 DC 9A E8 C7 DA D6 60 BB 80
```

```
              A5 E7 CE 85 53 D5 42 09 13 C2 A7 BA

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 B1 83 C9 90 2D 77 02 CE C4 C9 3D 5A 4E A8
           82 07 2F AF 5D BB C6 21 4B DC 31 35 7B DB 63 17 E8 92 02 20
           3A 73 92 26 60 C4 4D 08 45 A9 C5 99 15 0D B6 0B F5 12 78 AC
           16 F9 B9 57 2E B3 B1 55 AD EE 63 C3

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: 9C A4 C4 40 35 0F 2D 9C 56 1C 0B 4D 57 FE D7 CA A7 D3 BE BD


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: C5 B3 0E 5E 42 06 77 F1 F7 A8 C7 0B 92 05 F2 BB 07 DD 7F 41


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV+gAwIBAgIRAKROMOlG3VBw09iEa
+MYJKMwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA2MjYwNjM3Mz
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFJykxEA1Dy2cVhwLTVf
+18qn0769MB8GA1UdIwQYMBaAFMWzDl5CBnfx96jHC5IF8rsH3X9BMBIGA1UdEQEB/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 A4 4E 30 E9 46 DD 50 70 D3 D8 84 6B E3 18 24 A3

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:37:34 2024 GMT
Not Valid After: Jun 26 18:37:34 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 9D DE 08 6C A3 15 CB 7B 12 DC A4 50 6C 8F 08 57 2F 97 03 C6
              82 52 9C ED 9B 4A 67 48 4B DC 94 E2
Public Key Y: 1F 05 E0 44 18 1F 05 EB 08 F2 58 DC 9A E8 C7 DA D6 60 BB 80
```

```
              A5 E7 CE 85 53 D5 42 09 13 C2 A7 BA

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 B1 83 C9 90 2D 77 02 CE C4 C9 3D 5A 4E A8
           82 07 2F AF 5D BB C6 21 4B DC 31 35 7B DB 63 17 E8 92 02 20
           3A 73 92 26 60 C4 4D 08 45 A9 C5 99 15 0D B6 0B F5 12 78 AC
           16 F9 B9 57 2E B3 B1 55 AD EE 63 C3

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: 9C A4 C4 40 35 0F 2D 9C 56 1C 0B 4D 57 FE D7 CA A7 D3 BE BD


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: C5 B3 0E 5E 42 06 77 F1 F7 A8 C7 0B 92 05 F2 BB 07 DD 7F 41


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV+gAwIBAgIRAKROMOlG3VBw09iEa
+MYJKMwCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA2MjYwNjM3Mz
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFJykxEA1Dy2cVhwLTVf
+18qn0769MB8GA1UdIwQYMBaAFMWzDl5CBnfx96jHC5IF8rsH3X9BMBIGA1UdEQEB/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/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.
```

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.
```

17975 - Service Detection (GET 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 an HTTP request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/443/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  1.2.0  amd64  The installer of the Anapaya appliance.
  ii   anapaya-system-config  1.2.0  amd64  System configuration for Anapaya appliances.
  ii   apparmor  3.0.4-2ubuntu2.3  amd64  user-space parser utility for AppArmor
  ii   apt  2.4.11  amd64  commandline package manager
  ii   apt-transport-https  2.4.11  all  transitional package for https support
  ii   apt-utils  2.4.11  amd64  package management related utility programs
  ii   base-files  12ubuntu4.5  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  amd64  GNU Bourne Again SHell
  ii   bash-completion  1:2.11-5ubuntu1  all  programmable completion for the bash shell
  ii   bind9-dnsutils  1:9.18.18-0ubuntu0.22.04.2  amd64  Clients provided with BIND 9
  ii   bind9-host  1:9.18.18-0ubuntu0.22.04.2  amd64  DNS Lookup Utility
  ii   bind9-libs  1:9.18.18-0ubuntu0.22.04.2  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  amd64  extra utilities from 4.4BSD-Lite
  ii   bsdutils  1:2.37.2-4ubuntu3  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  2023031 [...]
```

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: 2024/06/24

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: 2024/04/24

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

```
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 192.168.111.1 :
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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 8 installs of XZ Utils:

  Path    : /var/lib/docker/
overlay2/45b66544ed5c326970a918cce54381d2f13425ff651d2e2be465e76e32ff195e/merged/bin/xz
  Version : unknown
  Path    : /var/lib/docker/
overlay2/23309494955c4fc69dc5251f118706e7f0fc1c53a138157c79da2405739a8c4a/diff/bin/xz
  Version : unknown

  Path              : /usr/bin/xz
  Version           : 5.2.5
  Associated Package : xz-utils 5.2.5-2ubuntu1
  Managed by OS     : True

  Path    : /var/lib/docker/
overlay2/3c86329df4320c1b47a513cdc60ec1085da1a207914b7b86a57c56c59a489295/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version : 5.2.5

  Path    : /var/lib/docker/overlay2/
b3600b6743c91d9dcb14a7404cd754575289bedccb84a3af2d971546524c5bab/diff/bin/xz
  Version : unknown

  Path    : /var/lib/docker/
overlay2/9c9663de679a078cdd688c98f096d27c8b6cc55aeabeeec625be30760168dd47/merged/lib/x86_64-linux-
gnu/liblzma.so.5.2.5
  Version : 5.2.5

  Path              : /usr/lib/x86_64-linux-gnu/liblzma.so.5.2.5
  Version           : 5.2.5
  Associated Package : liblzma5 5.2.5-2ubuntu1
  Managed by OS     : True

  Path    : /var/lib/docker/
overlay2/896946e081150cde1a2a1435da4bed3b1e76b47891c5bc7531234fc01c6fe2ae/diff/usr/lib/
liblzma.so.5.2.9
  Version : 5.2.9
```

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: 2024/05/31

Plugin Output

tcp/0

```
This machine is attached to an Ubuntu Pro subscription.

Binary Path                  : /var/lib/ubuntu-advantage
Binary Version               : 29.4~22.04

Enabled Ubuntu Pro Services  :
```

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 167172 12804 ?        Ss     2023 406:22 /lib/systemd/systemd --system --
deserialize 45 noquiet nosplash nofb
root           2  0.0  0.0      0     0 ?        S      2023   0:01 [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   4:16 [ksoftirqd/0]
root          14  0.0  0.0      0     0 ?        I      2023  85:16 [rcu_sched]
root          15  0.0  0.0      0     0 ?        S      2023   0:16 [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   0:17 [migration/1]
root          22  0.0  0.0      0     0 ?        S      2023   0:43 [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   0:14 [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: 2024/06/24

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: 2024/06/24

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 7.81.0-1ubuntu1.15
  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 7.81.0-1ubuntu1.15
  Managed by OS      : True
```

192.168.112.1

103	125	168	4	111
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jun 26 10:47:32 2024
End time:	Wed Jun 26 11:13:37 2024

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-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

7.7

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1l
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1o
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1p
```

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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.5
```

182319 - OpenSSL SEoL (1.1.0.x)

Synopsis

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

Description

According to its version, OpenSSL is 1.1.0.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/news/vulnerabilities-1.1.0.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/
overlay2/55741a7ec2d611d2f6666f1daf49cd84d2e2f02661f8e000cbdcfcda13f4d638/diff/usr/bin/openssl
  Installed version                     : 1.1.0l
  Security End of Life                  : September 12, 2019
  Time since Security End of Life (Est.) : >= 4 years
```

tcp/0

```
  Path                                   : /var/lib/docker/
overlay2/55741a7ec2d611d2f6666f1daf49cd84d2e2f02661f8e000cbdcfcda13f4d638/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Installed version                      : 1.1.0l
  Security End of Life                   : September 12, 2019
  Time since Security End of Life (Est.) : >= 4 years
```

tcp/0

```
  Path                                   : /var/lib/docker/
overlay2/55741a7ec2d611d2f6666f1daf49cd84d2e2f02661f8e000cbdcfcda13f4d638/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Installed version                      : 1.1.0l
  Security End of Life                   : September 12, 2019
  Time since Security End of Life (Est.) : >= 4 years
```

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/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/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Installed version                     : 1.1.1g
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/0fe44184e79c4674f36c21a1bc8e5663cf2639373e44b2780ca7c51acc9d3975/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/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Installed version                     : 1.1.1d
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Installed version                     : 1.1.1d
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Installed version                     : 1.1.1d
  Security End of Life                  : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                  : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Installed version                      : 1.1.1j
  Security End of Life                   : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                   : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Installed version                      : 1.1.1j
  Security End of Life                   : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                   : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/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/
overlay2/5bebb85d5d656eb7ac3812c25a40425e41cd4172ad92bdaf6eff8d5cdbc38512/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/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/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/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/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/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Installed version                      : 1.1.1d
  Security End of Life                   : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                   : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Installed version                      : 1.1.1j
  Security End of Life                   : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                   : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Installed version                      : 1.1.1d
  Security End of Life                   : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                   : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                      : 1.1.1d
  Security End of Life                   : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                   : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Installed version                      : 1.1.1d
  Security End of Life                   : September 11, 2023
  Time since Security End of Life (Est.) : >= 6 months
```

tcp/0

```
  Path                                   : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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
```

194474 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less vulnerability (USN-6756-1)

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 / 24.04 LTS. host has a package installed that is affected by a vulnerability as referenced in the USN-6756-1 advisory.

- less through 653 allows OS command execution via a newline character in the name of a file, because quoting is mishandled in filename.c. Exploitation typically requires use with attacker-controlled file names, such as the files extracted from an untrusted archive. Exploitation also requires the LESSOPEN environment variable, but this is set by default in many common cases. (CVE-2024-32487)

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-6756-1

Solution

Update the affected less package.

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

7.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-32487
XREF	USN:6756-1

Plugin Information

Published: 2024/04/29, Modified: 2024/04/29

Plugin Output

tcp/0

```
  - Installed package : less_590-1ubuntu0.22.04.2
  - Fixed package     : less_590-1ubuntu0.22.04.3
```

193362 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities (USN-6736-1)

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-6736-1 advisory.

- inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9840)

- inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic. (CVE-2016-9841)

- zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches. (CVE-2018-25032)

- zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference). (CVE-2022-37434)

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-6736-1

Solution

Update the affected klibc-utils, libklibc and / or libklibc-dev 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

6.7

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

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

References

CVE	CVE-2016-9840
CVE	CVE-2016-9841
CVE	CVE-2018-25032
CVE	CVE-2022-37434
XREF	USN:6736-1

Plugin Information

Published: 2024/04/16, Modified: 2024/04/16

Plugin Output

tcp/0

```
  - Installed package : klibc-utils_2.0.10-4
  - Fixed package     : klibc-utils_2.0.10-4ubuntu0.1

  - Installed package : libklibc_2.0.10-4
  - Fixed package     : libklibc_2.0.10-4ubuntu0.1
```

193515 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU C Library vulnerability (USN-6737-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6737-1 advisory.

- The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable. (CVE-2024-2961)

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-6737-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-2961
XREF	USN:6737-1

Plugin Information

Published: 2024/04/18, Modified: 2024/04/19

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.6
  - Fixed package     : libc-bin_2.35-0ubuntu3.7

  - Installed package : libc6_2.35-0ubuntu3.6
  - Fixed package     : libc6_2.35-0ubuntu3.7

  - Installed package : locales_2.35-0ubuntu3.6
  - Fixed package     : locales_2.35-0ubuntu3.7
```

180510 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6339-1)

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-6339-1 advisory.

- In the Linux kernel through 6.2.7, fs/ntfs3/inode.c has an invalid kfree because it does not validate MFT flags before replaying logs. (CVE-2022-48425)

- In multiple functions of binder.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. (CVE-2023-21255)

- There is a null-pointer-dereference flaw found in f2fs_write_end_io in fs/f2fs/data.c in the Linux kernel.

This flaw allows a local privileged user to cause a denial of service problem. (CVE-2023-2898)

- An issue was discovered in drivers/media/dvb-core/dvb_frontend.c in the Linux kernel 6.2. There is a blocking operation when a task is in !TASK_RUNNING. In dvb_frontend_get_event, wait_event_interruptible is called; the condition is dvb_frontend_test_event(fepriv,events). In dvb_frontend_test_event, down(&fepriv->sem) is called. However, wait_event_interruptible would put the process to sleep, and down(&fepriv->sem) may block the process. (CVE-2023-31084)

- A NULL pointer dereference issue was found in the gfs2 file system in the Linux kernel. It occurs on corrupt gfs2 file systems when the evict code tries to reference the journal descriptor structure after it has been freed and set to NULL. A privileged local user could use this flaw to cause a kernel panic.

(CVE-2023-3212)

- An issue was discovered in the Linux kernel before 6.3.4. ksmbd has an out-of-bounds read in smb2_find_context_vals when create_context's name_len is larger than the tag length. (CVE-2023-38426)

- An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/smb2pdu.c in ksmbd does not properly check the UserName value because it does not consider the address of security buffer, leading to an out- of-bounds read. (CVE-2023-38428)

- An issue was discovered in the Linux kernel before 6.3.4. fs/ksmbd/connection.c in ksmbd has an off-by-one error in memory allocation (because of ksmbd_smb2_check_message) that may lead to out-of-bounds access.

(CVE-2023-38429)

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-6339-1

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

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

VPR Score

6.7

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)

References

CVE	CVE-2022-48425
CVE	CVE-2023-2898
CVE	CVE-2023-3212
CVE	CVE-2023-21255
CVE	CVE-2023-31084
CVE	CVE-2023-38426
CVE	CVE-2023-38428
CVE	CVE-2023-38429
XREF	USN:6339-1

Plugin Information

Published: 2023/09/05, Modified: 2024/01/09

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-83-generic
 for this advisory.
```

182558 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6416-1)

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-6416-1 advisory.

- A hash collision flaw was found in the IPv6 connection lookup table in the Linux kernel's IPv6 functionality when a user makes a new kind of SYN flood attack. A user located in the local network or with a high bandwidth connection can increase the CPU usage of the server that accepts IPV6 connections up to 95%. (CVE-2023-1206)

- A side channel vulnerability on some of the AMD CPUs may allow an attacker to influence the return address prediction. This may result in speculative execution at an attacker-controlled address, potentially leading to information disclosure. (CVE-2023-20569)

- A flaw was found in the networking subsystem of the Linux kernel within the handling of the RPL protocol.

This issue results from the lack of proper handling of user-supplied data, which can lead to an assertion failure. This may allow an unauthenticated remote attacker to create a denial of service condition on the system. (CVE-2023-2156)

- A null pointer dereference flaw was found in the Linux kernel's DECnet networking protocol. This issue could allow a remote user to crash the system. (CVE-2023-3338)

- An issue was discovered in the Linux kernel before 6.3.10. fs/smb/server/smb2misc.c in ksmbd does not validate the relationship between the command payload size and the RFC1002 length specification, leading to an out-of-bounds read. (CVE-2023-38432)

- A use-after-free flaw was found in nfc_llcp_find_local in net/nfc/llcp_core.c in NFC in the Linux kernel.

This flaw allows a local user with special privileges to impact a kernel information leak issue.

(CVE-2023-3863)

- A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition. (CVE-2023-4132)

- A flaw was found in KVM AMD Secure Encrypted Virtualization (SEV) in the Linux kernel. A KVM guest using SEV-ES or SEV-SNP with multiple vCPUs can trigger a double fetch race condition vulnerability and invoke the `VMGEXIT` handler recursively. If an attacker manages to call the handler multiple times, they can trigger a stack overflow and cause a denial of service or potentially guest-to-host escape in kernel configurations without stack guard pages (`CONFIG_VMAP_STACK`). (CVE-2023-4155)

- A flaw was found in the Linux kernel's TUN/TAP functionality. This issue could allow a local user to bypass network filters and gain unauthorized access to some resources. The original patches fixing CVE-2023-1076 are incorrect or incomplete. The problem is that the following upstream commits - a096ccca6e50 (tun: tun_chr_open(): correctly initialize socket uid), - 66b2c338adce (tap: tap_open():

correctly initialize socket uid), pass inode->i_uid to sock_init_data_uid() as the last parameter and that turns out to not be accurate. (CVE-2023-4194)

- A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged attacker could use this flaw to overflow the kernel stack. (CVE-2023-4273)

- An issue was discovered in net/ceph/messenger_v2.c in the Linux kernel before 6.4.5. There is an integer signedness error, leading to a buffer overflow and remote code execution via HELLO or one of the AUTH frames. This occurs because of an untrusted length taken from a TCP packet in ceph_decode_32.

(CVE-2023-44466)

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-6416-1

Solution

Update the affected kernel package.

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

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

VPR Score

6.7

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

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

References

CVE	CVE-2023-1206
CVE	CVE-2023-2156

CVE	CVE-2023-3338
CVE	CVE-2023-3863
CVE	CVE-2023-3865
CVE	CVE-2023-3866
CVE	CVE-2023-4132
CVE	CVE-2023-4155
CVE	CVE-2023-4194
CVE	CVE-2023-4273
CVE	CVE-2023-20569
CVE	CVE-2023-38432
CVE	CVE-2023-44466
XREF	USN:6416-1

Plugin Information

Published: 2023/10/04, Modified: 2024/01/09

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-86-generic
 for this advisory.
```

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

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 5.15.0-79-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

6.7

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 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-102-
generic for this advisory.
```

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

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

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

Plugin Information

Published: 2024/03/29, 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     : 8.7.0
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/bin/curl
  Installed version : 7.64.0
  Fixed version     : 8.7.0
```

148402 - OpenSSL 1.1.1 < 1.1.1j Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

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

- The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23841)

- Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash.

OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i).

Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23840)

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?67f25180

http://www.nessus.org/u?78dabcb5

https://www.openssl.org/news/secadv/20210216.txt

https://www.cve.org/CVERecord?id=CVE-2021-23840

https://www.cve.org/CVERecord?id=CVE-2021-23841

Solution

Upgrade to OpenSSL version 1.1.1j 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

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

VPR Score

6.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2021-23840
CVE	CVE-2021-23841
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/04/09, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1j
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1j
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1j
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1j
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1j
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1j
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1j
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1j
```

148125 - OpenSSL 1.1.1 < 1.1.1k Multiple Vulnerabilities

Synopsis

The remote service is affected by multiple vulnerabilities.

Description

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

- The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a purpose has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named purpose values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions 1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k.

OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).

(CVE-2021-3450)

- An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j). (CVE-2021-3449)

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?144c950a

http://www.nessus.org/u?6aafb4b2

https://www.cve.org/CVERecord?id=CVE-2021-3449

https://www.cve.org/CVERecord?id=CVE-2021-3450

https://www.openssl.org/news/secadv/20210325.txt

Solution

Upgrade to OpenSSL version 1.1.1k or later.

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:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

7.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-3449
CVE	CVE-2021-3450
XREF	IAVA:2021-A-0149-S
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2021/03/25, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1k
  Path             : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1k
  Path             : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1k
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1k
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1k
```

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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1n
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1t
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1t
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

6.7

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
```

```
  Reported version : 1.1.1g
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1w
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1w
```

135919 - OpenSSL 1.1.1d < 1.1.1g Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

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

- Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the signature_algorithms_cert TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f). (CVE-2020-1967)

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?d80da51b

https://www.cve.org/CVERecord?id=CVE-2020-1967

https://www.openssl.org/news/secadv/20200421.txt

Solution

Upgrade to OpenSSL version 1.1.1g 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

4.4

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-2020-1967
XREF	IAVA:2020-A-0186-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/04/23, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1g
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1g
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1g
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1g
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1g
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1g
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1g
```

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

6.7

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

3.6

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.8
```

192219 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability (USN-6698-1)

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-6698-1 advisory.

- Vim before 9.0.2142 has a stack-based buffer overflow because did_set_langmap in map.c calls sprintf to write to the error buffer that is passed down to the option callback functions. (CVE-2024-22667)

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-6698-1

Solution

Update the affected packages.

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

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-2024-22667
XREF	USN:6698-1

Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

Plugin Output

tcp/0

```

  - Installed package : vim_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-common_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim-common_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-runtime_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim-runtime_2:8.2.3995-1ubuntu2.16

  - Installed package : vim-tiny_2:8.2.3995-1ubuntu2.15
  - Fixed package     : vim-tiny_2:8.2.3995-1ubuntu2.16

  - Installed package : xxd_2:8.2.3995-1ubuntu2.15
  - Fixed package     : xxd_2:8.2.3995-1ubuntu2.16

```

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

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
```

198244 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : GNU C Library vulnerabilities (USN-6804-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6804-1 advisory.

It was discovered that GNU C Library nscd daemon contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33599)

It was discovered that GNU C Library nscd daemon did not properly check the cache content, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33600)

It was discovered that GNU C Library nscd daemon did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service (system crash). (CVE-2024-33601)

It was discovered that GNU C Library nscd daemon did not properly handle memory allocation, which could lead to memory corruption. A local attacker could use this to cause a denial of service (system crash).

(CVE-2024-33602)

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-6804-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

5.5

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-33599
CVE	CVE-2024-33600
CVE	CVE-2024-33601
CVE	CVE-2024-33602
XREF	USN:6804-1

Plugin Information

Published: 2024/05/31, Modified: 2024/05/31

Plugin Output

tcp/0

```
  - Installed package : libc-bin_2.35-0ubuntu3.6
  - Fixed package     : libc-bin_2.35-0ubuntu3.8

  - Installed package : libc6_2.35-0ubuntu3.6
  - Fixed package     : libc6_2.35-0ubuntu3.8

  - Installed package : locales_2.35-0ubuntu3.6
  - Fixed package     : locales_2.35-0ubuntu3.8
```

198069 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Intel Microcode vulnerabilities (USN-6797-1)

Synopsis

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

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6797-1 advisory.

It was discovered that some 3rd and 4th Generation Intel Xeon Processors did not properly restrict access to certain hardware features when using Intel SGX or Intel TDX. This may allow a privileged local user to potentially further escalate their privileges on the system. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-22655)

It was discovered that some Intel Atom Processors did not properly clear register state when performing various operations. A local attacker could use this to obtain sensitive information via a transient execution attack. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-28746)

It was discovered that some Intel Processors did not properly clear the state of various hardware structures when switching execution contexts. A local attacker could use this to access privileged information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-38575)

It was discovered that some Intel Processors did not properly enforce bus lock regulator protections. A remote attacker could use this to cause a denial of service. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS. (CVE-2023-39368)

It was discovered that some Intel Xeon D Processors did not properly calculate the SGX base key when using Intel SGX. A privileged local attacker could use this to obtain sensitive information. This issue only affected Ubuntu 23.10, Ubuntu 22.04 LTS, Ubuntu 20.04 LTS, Ubuntu 18.04 LTS and Ubuntu 16.04 LTS.

(CVE-2023-43490)

It was discovered that some Intel Processors did not properly protect against concurrent accesses. A local attacker could use this to obtain sensitive information. (CVE-2023-45733)

It was discovered that some Intel Processors TDX module software did not properly validate input. A privileged local attacker could use this information to potentially further escalate their privileges on the system. (CVE-2023-45745, CVE-2023-47855)

It was discovered that some Intel Core Ultra processors did not properly handle particular instruction sequences. A local attacker could use this issue to cause a denial of service.

(CVE-2023-46103)

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-6797-1

Solution

Update the affected intel-microcode package.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22655
CVE	CVE-2023-28746
CVE	CVE-2023-38575
CVE	CVE-2023-39368
CVE	CVE-2023-43490
CVE	CVE-2023-45733
CVE	CVE-2023-45745
CVE	CVE-2023-46103
CVE	CVE-2023-47855
XREF	USN:6797-1

Plugin Information

Published: 2024/05/29, Modified: 2024/05/29

Plugin Output

tcp/0

```
  - Installed package : intel-microcode_3.20231114.0ubuntu0.22.04.1
  - Fixed package     : intel-microcode_3.20240514.0ubuntu0.22.04.1
```

193905 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : nghttp2 vulnerabilities (USN-6754-1)

Synopsis

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

Description

The remote Ubuntu 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-6754-1 advisory.

- Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both. (CVE-2019-9511)

- Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service.

The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU. (CVE-2019-9513)

- The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. (CVE-2023-44487)

- nghttp2 is an implementation of the Hypertext Transfer Protocol version 2 in C. The nghttp2 library prior to version 1.61.0 keeps reading the unbounded number of HTTP/2 CONTINUATION frames even after a stream is reset to keep HPACK context in sync. This causes excessive CPU usage to decode HPACK stream. nghttp2 v1.61.0 mitigates this vulnerability by limiting the number of CONTINUATION frames it accepts per stream.
There is no workaround for this vulnerability. (CVE-2024-28182)

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-6754-1

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

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

VPR Score

6.1

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

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

References

CVE	CVE-2019-9511
CVE	CVE-2019-9513
CVE	CVE-2023-44487
CVE	CVE-2024-28182
XREF	CISA-KNOWN-EXPLOITED:2023/10/31
XREF	USN:6754-1
XREF	CEA-ID:CEA-2024-0004
XREF	CEA-ID:CEA-2019-0643

Plugin Information

Published: 2024/04/25, Modified: 2024/04/26

Plugin Output

tcp/0

```
  - Installed package : libnghttp2-14_1.43.0-1ubuntu0.1
  - Fixed package     : libnghttp2-14_1.43.0-1ubuntu0.2
```

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

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 : libglib2.0-0_2.72.4-0ubuntu2.2
  - Fixed package     : libglib2.0-0_2.72.4-0ubuntu2.3

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

192621 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1)

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-6718-1 advisory.

- When a protocol selection parameter option disables all protocols without adding any then the default set of protocols would remain in the allowed set due to an error in the logic for removing protocols. The below command would perform a request to curl.se with a plaintext protocol which has been explicitly disabled. curl --proto -all,-http http://curl.se The flaw is only present if the set of selected protocols disables the entire set of available protocols, in itself a command with no practical use and therefore unlikely to be encountered in real situations. The curl security team has thus assessed this to be low severity bug. (CVE-2024-2004)

- 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.

(CVE-2024-2398)

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-6718-1

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

4.4

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-2024-2004
CVE	CVE-2024-2398
XREF	USN:6718-1
XREF	IAVA:2024-A-0185

Plugin Information

Published: 2024/03/27, Modified: 2024/03/29

Plugin Output

tcp/0

```
  - Installed package : curl_7.81.0-1ubuntu1.15
  - Fixed package     : curl_7.81.0-1ubuntu1.16

  - Installed package : libcurl3-gnutls_7.81.0-1ubuntu1.15
  - Fixed package     : libcurl3-gnutls_7.81.0-1ubuntu1.16

  - Installed package : libcurl4_7.81.0-1ubuntu1.15
  - Fixed package     : libcurl4_7.81.0-1ubuntu1.16
```

191019 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : libxml2 vulnerability (USN-6658-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6658-1 advisory.

- An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free. (CVE-2024-25062)

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-6658-1

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

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

VPR Score

4.4

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

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

STIG Severity

II

References

CVE	CVE-2024-25062
XREF	IAVA:2024-A-0067
XREF	USN:6658-1

Plugin Information

Published: 2024/02/26, Modified: 2024/03/11

Plugin Output

tcp/0

```
  - Installed package : libxml2_2.9.13+dfsg-1ubuntu0.3
  - Fixed package     : libxml2_2.9.13+dfsg-1ubuntu0.4
```

192629 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-1 advisory.

- wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover. (CVE-2024-28085)

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-6719-1

Solution

Update the affected packages.

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

7.9

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

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

References

CVE	CVE-2024-28085
XREF	USN:6719-1

Plugin Information

Published: 2024/03/27, Modified: 2024/03/29

Plugin Output

tcp/0

```
  - Installed package : bsdextrautils_2.37.2-4ubuntu3
  - Fixed package     : bsdextrautils_2.37.2-4ubuntu3.3

  - Installed package : bsdutils_1:2.37.2-4ubuntu3
  - Fixed package     : bsdutils_1:2.37.2-4ubuntu3.3

  - Installed package : eject_2.37.2-4ubuntu3
  - Fixed package     : eject_2.37.2-4ubuntu3.3

  - Installed package : fdisk_2.37.2-4ubuntu3
  - Fixed package     : fdisk_2.37.2-4ubuntu3.3

  - Installed package : libblkid1_2.37.2-4ubuntu3
  - Fixed package     : libblkid1_2.37.2-4ubuntu3.3

  - Installed package : libfdisk1_2.37.2-4ubuntu3
  - Fixed package     : libfdisk1_2.37.2-4ubuntu3.3

  - Installed package : libmount1_2.37.2-4ubuntu3
  - Fixed package     : libmount1_2.37.2-4ubuntu3.3

  - Installed package : libsmartcols1_2.37.2-4ubuntu3
  - Fixed package     : libsmartcols1_2.37.2-4ubuntu3.3

  - Installed package : libuuid1_2.37.2-4ubuntu3
  - Fixed package     : libuuid1_2.37.2-4ubuntu3.3

  - Installed package : mount_2.37.2-4ubuntu3
  - Fixed package     : mount_2.37.2-4ubuntu3.3

  - Installed package : util-linux_2.37.2-4ubuntu3
  - Fixed package     : util-linux_2.37.2-4ubuntu3.3
```

193159 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-2)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6719-2 advisory.

- wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover. (CVE-2024-28085)

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-6719-2

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.9

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28085
XREF	USN:6719-2

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : bsdextrautils_2.37.2-4ubuntu3
  - Fixed package     : bsdextrautils_2.37.2-4ubuntu3.4

  - Installed package : bsdutils_1:2.37.2-4ubuntu3
  - Fixed package     : bsdutils_1:2.37.2-4ubuntu3.4

  - Installed package : eject_2.37.2-4ubuntu3
  - Fixed package     : eject_2.37.2-4ubuntu3.4

  - Installed package : fdisk_2.37.2-4ubuntu3
  - Fixed package     : fdisk_2.37.2-4ubuntu3.4

  - Installed package : libblkid1_2.37.2-4ubuntu3
  - Fixed package     : libblkid1_2.37.2-4ubuntu3.4

  - Installed package : libfdisk1_2.37.2-4ubuntu3
  - Fixed package     : libfdisk1_2.37.2-4ubuntu3.4

  - Installed package : libmount1_2.37.2-4ubuntu3
  - Fixed package     : libmount1_2.37.2-4ubuntu3.4

  - Installed package : libsmartcols1_2.37.2-4ubuntu3
  - Fixed package     : libsmartcols1_2.37.2-4ubuntu3.4

  - Installed package : libuuid1_2.37.2-4ubuntu3
  - Fixed package     : libuuid1_2.37.2-4ubuntu3.4

  - Installed package : mount_2.37.2-4ubuntu3
  - Fixed package     : mount_2.37.2-4ubuntu3.4

  - Installed package : util-linux_2.37.2-4ubuntu3
  - Fixed package     : util-linux_2.37.2-4ubuntu3.4
```

180259 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6315-1)

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-6315-1 advisory.

- Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. (CVE-2022-40982)

- An issue in Zen 2 CPUs, under specific microarchitectural circumstances, may allow an attacker to potentially access sensitive information. (CVE-2023-20593)

- In multiple functions of io_uring.c, there is a possible kernel memory corruption due to improper locking.

This could lead to local escalation of privilege in the kernel with System execution privileges needed.

User interaction is not needed for exploitation. (CVE-2023-21400)

- A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, u32_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 04c55383fa5689357bcdd2c8036725a55ed632bc.

(CVE-2023-3609)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Flaw in the error handling of bound chains causes a use-after-free in the abort path of NFT_MSG_NEWRULE. The vulnerability requires CAP_NET_ADMIN to be triggered. We recommend upgrading past commit 4bedf9eee016286c835e3d8fa981ddece5338795. (CVE-2023-3610)

- An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The qfq_change_agg() function in net/sched/sch_qfq.c allows an out- of-bounds write because lmax is updated according to packet sizes without bounds checks. We recommend upgrading past commit 3e337087c3b5805fe0b8a46ba622a962880b5d64. (CVE-2023-3611)

- A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, fw_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 0323bce598eea038714f941ce2b22541c46d488f.

(CVE-2023-3776)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. When nf_tables_delrule() is flushing table rules, it is not checked whether the chain is bound and the chain's owner rule can also release the objects in certain circumstances. We recommend upgrading past commit 6eaf41e87a223ae6f8e7a28d6e78384ad7e407f8.

(CVE-2023-3777)

- Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority because it is a duplicate of CVE-2023-4147. (CVE-2023-3995)

- A use-after-free flaw was found in the Linux kernel's netfilter in the way a user triggers the nft_pipapo_remove function with the element, without a NFT_SET_EXT_KEY_END. This issue could allow a local user to crash the system or potentially escalate their privileges on the system. (CVE-2023-4004)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. On an error when building a nftables rule, deactivating immediate expressions in nft_immediate_deactivate() can lead unbinding the chain and objects be deactivated but later used. We recommend upgrading past commit 0a771f7b266b02d262900c75f1e175c7fe76fec2. (CVE-2023-4015)

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-6315-1

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

7.1

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-2022-40982

CVE	CVE-2023-3609
CVE	CVE-2023-3610
CVE	CVE-2023-3611
CVE	CVE-2023-3776
CVE	CVE-2023-3777
CVE	CVE-2023-3995
CVE	CVE-2023-4004
CVE	CVE-2023-4015
CVE	CVE-2023-20593
CVE	CVE-2023-21400
XREF	USN:6315-1

Plugin Information

Published: 2023/08/29, Modified: 2024/01/09

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-82-generic
 for this advisory.
```

181635 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6386-1)

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-6386-1 advisory.

- A division-by-zero error on some AMD processors can potentially return speculative data resulting in loss of confidentiality. (CVE-2023-20588)

- An issue was discovered in l2cap_sock_release in net/bluetooth/l2cap_sock.c in the Linux kernel before 6.4.10. There is a use-after-free because the children of an sk are mishandled. (CVE-2023-40283)

- A memory leak flaw was found in nft_set_catchall_flush in net/netfilter/nf_tables_api.c in the Linux Kernel. This issue may allow a local attacker to cause double-deactivations of catchall elements, which can result in a memory leak. (CVE-2023-4569)

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-6386-1

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

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-2023-4128
CVE	CVE-2023-4569
CVE	CVE-2023-20588
CVE	CVE-2023-40283
XREF	USN:6386-1

Plugin Information

Published: 2023/09/19, Modified: 2024/01/09

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-84-generic
 for this advisory.
```

183454 - Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6446-1)

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-6446-1 advisory.

- The fix for XSA-423 added logic to Linux'es netback driver to deal with a frontend splitting a packet in a way such that not all of the headers would come in one piece. Unfortunately the logic introduced there didn't account for the extreme case of the entire packet being split into as many pieces as permitted by the protocol, yet still being smaller than the area that's specially dealt with to keep all (possible) headers together. Such an unusual packet would therefore trigger a buffer overrun in the driver.

(CVE-2023-34319)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Due to a race condition between nf_tables netlink control plane transaction and nft_set element garbage collection, it is possible to underflow the reference counter causing a use-after-free vulnerability. We recommend upgrading past commit 3e91b0ebd994635df2346353322ac51ce84ce6d8. (CVE-2023-4244)

- An integer overflow flaw was found in the Linux kernel. This issue leads to the kernel allocating `skb_shared_info` in the userspace, which is exploitable in systems without SMAP protection since `skb_shared_info` contains references to function pointers. (CVE-2023-42752)

- An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could lead to a miscalculation of the `h->nets` array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system. (CVE-2023-42753)

- A flaw was found in the IPv4 Resource Reservation Protocol (RSVP) classifier in the Linux kernel. The xprt pointer may go beyond the linear part of the skb, leading to an out-of-bounds read in the `rsvp_classify` function. This issue may allow a local user to crash the system and cause a denial of service.

(CVE-2023-42755)

- A flaw was found in the Netfilter subsystem of the Linux kernel. A race condition between IPSET_CMD_ADD and IPSET_CMD_SWAP can lead to a kernel panic due to the invocation of `__ip_set_put` on a wrong `set`.

This issue may allow a local user to crash the system. (CVE-2023-42756)

- A use-after-free vulnerability in the Linux kernel's af_unix component can be exploited to achieve local privilege escalation. The unix_stream_sendpage() function tries to add data to the last skb in the peer's recv queue without locking the queue. Thus there is a race where unix_stream_sendpage() could access an skb locklessly that is being released by garbage collection, resulting in use-after-free. We recommend upgrading past commit 790c2f9d15b594350ae9bca7b236f2b1859de02c. (CVE-2023-4622)

- A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploited to achieve local privilege escalation. If a class with a link-sharing curve (i.e. with the HFSC_FSC flag set) has a parent without a link-sharing curve, then init_vf() will call vttree_insert() on the parent, but vttree_remove() will be skipped in update_vf(). This leaves a dangling pointer that can cause a use-after-free. We recommend upgrading past commit b3d26c5702c7d6c45456326e56d2ccf3f103e60f. (CVE-2023-4623)

- Rejected reason: CVE-2023-4881 was wrongly assigned to a bug that was deemed to be a non-security issue by the Linux kernel security team. (CVE-2023-4881)

- A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. When the plug qdisc is used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect .peek handler of sch_plug and lack of error checking in agg_dequeue(). We recommend upgrading past commit 8fc134fee27f2263988ae38920bc03da416b03d8. (CVE-2023-4921)

- A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Addition and removal of rules from chain bindings within the same transaction causes leads to use-after-free. We recommend upgrading past commit f15f29fd4779be8a418b66e9d52979bb6d6c2325. (CVE-2023-5197)

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-6446-1

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

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-2023-4244
CVE	CVE-2023-4622
CVE	CVE-2023-4623
CVE	CVE-2023-4881
CVE	CVE-2023-4921
CVE	CVE-2023-5197
CVE	CVE-2023-34319
CVE	CVE-2023-42752
CVE	CVE-2023-42753
CVE	CVE-2023-42755
CVE	CVE-2023-42756
XREF	USN:6446-1

Plugin Information

Published: 2023/10/20, Modified: 2024/01/09

Plugin Output

tcp/0

```
Running Kernel level of 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-87-generic
 for this advisory.
```

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

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 5.15.0-79-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

8.4

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 5.15.0-79-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

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 5.15.0-79-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

6.7

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 5.15.0-79-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

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 5.15.0-79-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

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 5.15.0-79-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

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 5.15.0-79-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

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 5.15.0-79-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

6.7

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 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-112-
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

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
```

200099 - Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : libarchive vulnerability (USN-6805-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6805-1 advisory.

It was discovered that libarchive incorrectly handled certain RAR archive files. An attacker could possibly use this issue to execute arbitrary code or cause a crash.

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-6805-1

Solution

Update the affected packages.

Risk Factor

High

CVSS v3.0 Base Score

7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/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

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-26256
XREF	USN:6805-1

Plugin Information

Published: 2024/06/04, Modified: 2024/06/04

Plugin Output

tcp/0

```
  - Installed package : libarchive13_3.6.0-1ubuntu1
  - Fixed package     : libarchive13_3.6.0-1ubuntu1.1
```

192198 - Ubuntu 22.04 LTS : Bash vulnerability (USN-6697-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 22.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6697-1 advisory.

- A flaw was found in the bash package, where a heap-buffer overflow can occur in valid parameter_transform.

This issue may lead to memory problems. (CVE-2022-3715)

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-6697-1

Solution

Update the affected bash, bash-builtins and / or bash-static packages.

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

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-2022-3715
XREF	USN:6697-1

Plugin Information

Published: 2024/03/18, Modified: 2024/03/18

Plugin Output

tcp/0

```
  - Installed package : bash_5.1-6ubuntu1
  - Fixed package     : bash_5.1-6ubuntu1.1
```

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

6.3

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

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
```

200200 - OpenSSL 1.1.1 < 1.1.1e Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

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

- There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t). (CVE-2019-1551)

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?d01cae2c

https://www.cve.org/CVERecord?id=CVE-2019-1551

https://www.openssl.org/news/secadv/20191206.txt

Solution

Upgrade to OpenSSL version 1.1.1e 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

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-2019-1551
XREF	IAVA:2019-A-0303-S

Plugin Information

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

Plugin Output

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1e
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1e
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1e
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
```

```
  Reported version : 1.1.1d
  Fixed version    : 1.1.1e
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1e
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1e
```

tcp/0

```

  Path             : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1e
```

144047 - OpenSSL 1.1.1 < 1.1.1i Vulnerability

Synopsis

The remote service is affected by a vulnerability.

Description

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

- The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified.

OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue.

Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971)

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?1f13c66b

https://www.cve.org/CVERecord?id=CVE-2020-1971

https://www.openssl.org/news/secadv/20201208.txt

Solution

Upgrade to OpenSSL version 1.1.1i 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

6.1

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-2020-1971
XREF	IAVA:2020-A-0566-S
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025

Plugin Information

Published: 2020/12/10, Modified: 2024/06/07

Plugin Output

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1i
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
```

```
  Reported version : 1.1.1d
  Fixed version    : 1.1.1i
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1i
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1i
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1i
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1i
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1i
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1i
```

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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
```

```
  Reported version : 1.1.1d
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1m
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1q
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
```

```
  Reported version : 1.1.1j
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1u
```

tcp/0

```

  Path             : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1u
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

2.9

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1v
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1v
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/0fe44184e79c4674f36c21a1bc8e5663cf2639373e44b2780ca7c51acc9d3975/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/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5bebb85d5d656eb7ac3812c25a40425e41cd4172ad92bdaf6eff8d5cdbc38512/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/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1x
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1x
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1x
```

tcp/0

```

  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

5.9

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/
overlay2/046a12b46bfd029a0c4d9fb7ce14f969ad5288c79b81812479be60a603fc4451/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/0799e78ac2cd9e8361787fd08250988f0ebf82144345b2bf203269888a457fb8/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1g
  Fixed version    : 1.1.1y
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/0fe44184e79c4674f36c21a1bc8e5663cf2639373e44b2780ca7c51acc9d3975/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/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1y
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/1d0e7ae066566bcfd60ed7fcd20a74d84ede1dca97f53180ccc0de267088ba51/diff/usr/lib/x86_64-linux-
gnu/libcrypto.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1y
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/1ecf70b62d8df3477dba7a849aa7ce28277a595218fdd9cfffa718a2ac4658b5/diff/usr/lib/x86_64-linux-
gnu/libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1y
```

tcp/0

```

  Path              : /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/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/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/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/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libcrypto.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/lib/libssl.so.1.1
  Reported version : 1.1.1j
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/56f671460d71a60745ed2a69282980fdf5b50e504ad348e4133ed6a0b132f75c/diff/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/5bebb85d5d656eb7ac3812c25a40425e41cd4172ad92bdaf6eff8d5cdbc38512/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/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/
overlay2/6f487e85f0a87fedfce9eb87a12937d76baee717a27ca7e54bd70a61b366cd4b/diff/lib/libssl.so.1.1
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/739a15d975dfe8dc645d898e22351d270e8a9a4edf2b74d8a2f939987b3dff8c/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/7bf9bb1461785ac2f3da6715f2312352ba41d3062b49f96e04c0433cfa71cc18/diff/usr/bin/openssl
  Reported version : 1.1.1j
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/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/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/bin/openssl
  Reported version : 1.1.1d
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path             : /var/lib/docker/overlay2/
d1d7521d106a0ca36239b8634c790070287e4c4f656e818f20dd8305712cdb0a/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
e9ca40f1e359bd1e9903dd1eab06b5928f623a4b27beb3534056513e20b401f4/diff/usr/lib/x86_64-linux-gnu/
libssl.so.1.1
  Reported version : 1.1.1d
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged/usr/bin/openssl
  Reported version : 1.1.1k
  Fixed version    : 1.1.1y
```

tcp/0

```
  Path              : /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/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

2.9

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

5.9

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/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

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/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged/usr/lib/x86_64-linux-gnu/
libcrypto.so.3
  Reported version : 3.0.2
  Fixed version    : 3.0.9
```

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
```

198044 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2 vulnerability (USN-6787-1)

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 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6787-1 advisory.

It was discovered that Jinja2 incorrectly handled certain HTML attributes that were accepted by the xmlattr filter. An attacker could use this issue to inject arbitrary HTML attribute keys and values to potentially execute a cross-site scripting (XSS) attack.

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-6787-1

Solution

Update the affected python-jinja2 and / or python3-jinja2 packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.3

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

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

References

CVE	CVE-2024-34064
XREF	USN:6787-1

Plugin Information

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

Plugin Output

tcp/0

```
  - Installed package : python3-jinja2_3.0.3-1ubuntu0.1
  - Fixed package     : python3-jinja2_3.0.3-1ubuntu0.2
```

200307 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF vulnerability (USN-6827-1)

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 / 24.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-6827-1 advisory.

It was discovered that LibTIFF incorrectly handled memory when

performing certain cropping operations, leading to a heap buffer overflow. An attacker could use this issue to cause a

denial of service, or possibly execute arbitrary code.

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-6827-1

Solution

Update the affected packages.

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

3.6

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-2023-3164
XREF	USN:6827-1

Plugin Information

Published: 2024/06/11, Modified: 2024/06/11

Plugin Output

tcp/0

```
  - Installed package : libtiff5_4.3.0-6ubuntu0.8
  - Fixed package     : libtiff5_4.3.0-6ubuntu0.9
```

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

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

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.
```

197569 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : idna vulnerability (USN-6780-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 16.04 LTS / 18.04 LTS / 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-6780-1 advisory.

Guido Vranken discovered that idna did not properly manage certain inputs,

which could lead to significant resource consumption. 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-6780-1

Solution

Update the affected pypy-idna, python-idna and / or python3-idna 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:N/I:N/A:H)

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-3651
XREF	USN:6780-1

Plugin Information

Published: 2024/05/21, Modified: 2024/05/23

Plugin Output

tcp/0

```
  - Installed package : python3-idna_3.3-1
  - Fixed package     : python3-idna_3.3-1ubuntu0.1
```

198063 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : TPM2 Software Stack vulnerabilities (USN-6796-1)

Synopsis

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

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-6796-1 advisory.

Fergus Dall discovered that TPM2 Software Stack did not properly handle layer arrays. An attacker could possibly use this issue to cause

TPM2 Software Stack to crash, resulting in a denial of service, or

possibly execute arbitrary code. (CVE-2023-22745)

Jurgen Repp and Andreas Fuchs discovered that TPM2 Software Stack did not

validate the quote data after deserialization. An attacker could generate an arbitrary quote and cause TPM2 Software Stack to have unknown behavior.

(CVE-2024-29040)

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-6796-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

5.9 (CVSS2#AV:L/AC:H/Au:M/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-22745
CVE	CVE-2024-29040
XREF	USN:6796-1

Plugin Information

Published: 2024/05/29, Modified: 2024/05/29

Plugin Output

tcp/0

```
  - Installed package : libtss2-esys-3.0.2-0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-esys-3.0.2-0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-mu0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-mu0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-sys1_3.2.0-1ubuntu1
  - Fixed package     : libtss2-sys1_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-cmd0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-cmd0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-device0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-device0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-mssim0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-mssim0_3.2.0-1ubuntu1.1

  - Installed package : libtss2-tcti-swtpm0_3.2.0-1ubuntu1
  - Fixed package     : libtss2-tcti-swtpm0_3.2.0-1ubuntu1.1
```

194475 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GNU cpio vulnerabilities (USN-6755-1)

Synopsis

The remote Ubuntu host is missing a security update.

Description

The remote Ubuntu 20.04 LTS / 22.04 LTS / 23.10 host has packages installed that are affected by a vulnerability as referenced in the USN-6755-1 advisory.

- Debian's cpio contains a path traversal vulnerability. This issue was introduced by reverting CVE-2015-1197 patches which had caused a regression in --no-absolute-filenames. Upstream has since provided a proper fix to --no-absolute-filenames. (CVE-2023-7207)

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-6755-1

Solution

Update the affected cpio and / or cpio-win32 packages.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

3.6

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2023-7207
XREF	USN:6755-1

Plugin Information

Published: 2024/04/29, Modified: 2024/04/29

Plugin Output

tcp/0

```
  - Installed package : cpio_2.13+dfsg-7
  - Fixed package     : cpio_2.13+dfsg-7ubuntu0.1
```

193341 - Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : GnuTLS vulnerabilities (USN-6733-1)

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-6733-1 advisory.

- A flaw was found in GnuTLS. The Minerva attack is a cryptographic vulnerability that exploits deterministic behavior in systems like GnuTLS, leading to side-channel leaks. In specific scenarios, such as when using the GNUTLS_PRIVKEY_FLAG_REPRODUCIBLE flag, it can result in a noticeable step in nonce size from 513 to 512 bits, exposing a potential timing side-channel. (CVE-2024-28834)

- A flaw has been discovered in GnuTLS where an application crash can be induced when attempting to verify a specially crafted .pem bundle using the certtool --verify-chain command. (CVE-2024-28835)

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-6733-1

Solution

Update the affected packages.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

References

CVE	CVE-2024-28834
CVE	CVE-2024-28835
XREF	USN:6733-1

Plugin Information

Published: 2024/04/15, Modified: 2024/04/15

Plugin Output

tcp/0

```
  - Installed package : libgnutls30_3.7.3-4ubuntu1.4
  - Fixed package     : libgnutls30_3.7.3-4ubuntu1.5
```

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

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 5.15.0-79-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

6.7

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 5.15.0-79-generic does not meet the minimum fixed level of 5.15.0-107-
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

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 difference between the local and remote clocks is -2 seconds.
```

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

2.2

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: 2024/06/24

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: 2024/06/24

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:25.0.3 -> 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:openssl:openssl:1.1.0l -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:1.1.1d -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:1.1.1g -> OpenSSL Project OpenSSL
    cpe:/a:openssl:openssl:1.1.1j -> OpenSSL Project OpenSSL
    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:51ig -> OpenSSL Project OpenSSL
    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:5.2.9 -> 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: 2024/06/24

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 7.81.0-1ubuntu1.15
    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: 2024-06-26 08:48:59
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: 2024/06/24

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: 2024/06/24

Plugin Output

tcp/0

```
Docker container bda20d07e2dd3d06a5d99d7eadae5e0db8ede442c32ec4e956a0274eb2b6b2b9 has 7 changed
 files

Docker container f4f0dcde2323a96bd27cfbeb4b704c6b9d7041f477f73a73ea39afe4b5f31122 has 18 changed
 files

Docker container 61775e3c4a5b29e5977757e867a3507677da07654cec37cfe1075b2d827c9c18 has 6 changed
 files

Docker container 972fb5a7a50713cdeda414240497577420d6d8a229409b99a96c1a31d6953c89 has 9 changed
 files

Docker container c589bbace95332873cf3902573342e0994de7139b489db162dc98498e8b22528 has 3 changed
 files

Docker container ebb452ce48b808628eab5142263c556e0b28c20508c3067951a54b67ec41dfd7 has 5 changed
 files

Docker container d68a638a9c90a4092fc301b0d95e9bd38664dd411e26f5683f5422675552f89f has 6 changed
 files

Docker container 6b04447a877145f8e527b677e43c45244f9a5c3ce1fc6523faa46a5df1fcd5f4 has 14 changed
 files
```

```
Docker container 193b749ad7527ff8006d155ff8b1010e9e1ac7310abf7f786c016ba098df364a has 6 changed
 files

Docker container 520278ad1251f66d24dba30eb8016394c530e025d77dae3028d176ed022ad5f3 has 6 changed
 files

Docker container a2d62690b8ba2c6e874e778f2a38a8bf40717d3b11b2dcb1fab1e2ac2553663a has 26 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: 2024/06/24

Plugin Output

tcp/0

```
  Path    : /usr/bin/docker
  Version : 25.0.3
  build   : 4debf41
```

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: 2024/06/24

Plugin Output

tcp/0

```
  Version: 25.0.3
  Version: 25.0.3
  Version: 1.6.28
  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:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
Tag:       v0.35.4
ID:        bda20d07e2dd3d06a5d99d7eadae5e0db8ede442c32ec4e956a0274eb2b6b2b9
Ports:     n/a

Name:      /dataplane
Image:     vpp-dataplane
Image ID : sha256:2713bb13f7dd53ef4823583e7335fba2f066508afd00380bcff049576934959f
Tag:       v0.35.4
ID:        f4f0dcde2323a96bd27cfbeb4b704c6b9d7041f477f73a73ea39afe4b5f31122
Ports:     n/a

Name:      /router
Image:     scion-all
```

```
Image ID : sha256:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
Tag:       v0.35.4
ID:        61775e3c4a5b29e5977757e867a3507677da07654cec37cfe1075b2d827c9c18
Ports:     n/a

Name:      /appliance-cron
Image:     appliance
Image ID : sha256:104f6bcef2cddf5c1f33eff96cbe0601992a8e518ec7ed599913688f3b966f5c
Tag:       v0.35.4
ID:        972fb5a7a50713cdeda414240497577420d6d8a229409b99a96c1a31d6953c89
Ports:     n/a

Name:      /telemetry
Image:     opentelemetry-collector
Image ID : sha256:bb0d0d8b3897adeafdda039a41065799747ac0e87ce3d36fe1fd058922fe7732
Tag:       v0.35.4
ID:        c589bbace95332873cf3902573342e0994de7139b489db162dc98498e8b22528
Ports:     n/a

Name:      /node-exporter
Image:     node-exporter
Image ID : sha256:343b79e8fe11cee57367c06f6391c7ce118871a3ec6c3d291369c734ffd91ee1
Tag:       v0.35.4
ID:        ebb452ce48b808628eab5142263c556e0b28c20508c3067951a54b67ec41dfd7
Ports:     n/a

Name:      /promtail
Image:     promtail
Image ID : sha256:98b1e36a7b1304ae98e571ee63cfba659ff95bb6e579c18694f2979a7f9071e4
Tag:       v0.35.4
ID:        d68a638a9c90a4092fc301b0d95e9bd38664dd411e26f5683f5422675552f89f
Ports:     n/a

Name:      /daemon-64-2_0_2d
Image:     scion-all
Image ID : sha256:dfa060592f3fdf8f03297b981e70d80e1d685c9b835ce2edbcb019acef5ae093
Tag:       v0.35.4
ID:        6b04447a877145f8e52 [...]
```

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: 2024/06/24

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::bede:49c7:42c5:8966 (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)
  - 02:42:1c:46:aa:4d (interface docker0)
  - 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)
  - 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::bede:49c7:42c5:8966
        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 : 02:42:1c:46:aa:4d
  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: 2024/06/24

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
  - 02:42:1C:46:AA:4D
  - 00:90:0B:A5:D2:93
  - 00:90:0B:A5:D2:8E
  - 00:90:0B:A5:D2:90
  - 00:90:0B:A5:D2:92
  - 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: 2021/05/19

Plugin Output

tcp/443/www

```

  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
```

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/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: Wed, 26 Jun 2024 08:55:59 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: Wed, 26 Jun 2024 08:55:59 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: Wed, 26 Jun 2024 08:55:59 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: 2024/06/24

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
+ i.ABAAAAQAAAAC2
+ scion-gateway
  + IPv6
    - Address       : fe80::bede:49c7:42c5:8966
      Assign Method : static
```

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: 2024/06/24

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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 30 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/
overlay2/0fe44184e79c4674f36c21a1bc8e5663cf2639373e44b2780ca7c51acc9d3975/merged/usr/lib/x86_64-
linux-gnu/libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/0fe44184e79c4674f36c21a1bc8e5663cf2639373e44b2780ca7c51acc9d3975/merged/usr/lib/x86_64-
linux-gnu/libgcrypt.so.20.2.8
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/487592c2b6545575ef3bb2e82f706b3211dc1793ae9cdefcee621da571807d08/diff/usr/lib/x86_64-linux-
gnu/libgcrypt.so.20
  Version : 1.8.8

  Path    : /var/lib/docker/
overlay2/487592c2b6545575ef3bb2e82f706b3211dc1793ae9cdefcee621da571807d08/diff/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

  P [...]
```

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   19G   28G  40% /
tmpfs                             3.9G     0  3.9G   0% /dev/shm
tmpfs                             5.0M     0  5.0M   0% /run/lock
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/852bf32bb368f3889bcd84da8dfa1844041a05027fe81936cf2ab5fa6d5db2a4/merged
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/17313bdc9b7a8e2fdf17602e7eba9c1a31f9cd257d0dfe2c0bb46800cdeb621c/merged
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/40fc09f53847c67d6202a2c97a7903700a0d8a6729afdd9aa1b5c823ab2ab69f/merged
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/6aa7154827a741c75232e244706bd0590541a6f4f1ac99a2792e52fbc064cc1d/merged
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/0fe44184e79c4674f36c21a1bc8e5663cf2639373e44b2780ca7c51acc9d3975/merged
overlay                            49G   19G   28G  40% /var/lib/docker/overlay2/
fafb87344dd711fe1ff7b409d51d239e5e8abef5cd13428191efcec74beec056/merged
overlay                            49G   19G   28G  40% /var/lib/docker/overlay2/
e2c734e730391f8c0232a402afd5d9ed2c3cc86247b5737a5130d7c5da3dd693/merged
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/32bc3230acb4e9f2ad343ea2b3b302d3b72ba69b09c568ab1629b2c00022c0a5/merged
overlay                            49G   19G   28G  40% /var/lib/docker/overlay2/
e3fc31e4ae4ae00c1f87be4aa27317306b15a2c752e6dc498037982e497a45ff/merged
```

```
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/6a32edeba18d4beed3b9d2adbb4983e3d6a4bd8b29a49db13bfe016899b4b58b/merged
overlay                            49G   19G   28G  40% /var/lib/docker/
overlay2/156cfd1954961e41c2c20bb03e52deb2f8d4f19714892622657517bb686234ee/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
               docker
               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
  [...]
```

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: 2024/06/04

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.7.4
Nessus build : 20055
Plugin feed version : 202406250936
Scanner edition used : Nessus
Scanner OS : LINUX
Scanner distribution : ubuntu1404-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 : 54.905 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 : 2024/6/26 10:47 CEST
Scan duration : 1552 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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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: If the scan policy has WMI Netstat enabled, 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: 2024/04/24

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 daemon is not managed by dpkg :

/usr/local/bin/appliance
```

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 5.15.0-79-generic on Ubuntu 22.04
Confidence level : 100
Method : LinuxDistribution


The remote host is running Linux Kernel 5.15.0-79-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 5.15.0-79-generic #86-Ubuntu SMP Mon Jul 10 16:07:21 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 : 26.220207 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: 2024/06/24

Plugin Output

tcp/22/ssh

```
  Service : ssh
  Version : 8.9p1
  Banner  : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6
```

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: 2024/06/11

Plugin Output

tcp/0

```
. You need to take the following 46 actions :

[ Curl 7.44.0 < 8.7.0 HTTP/2 Push Headers Memory-leak (CVE-2024-2398) (192704) ]

+ Action to take : Upgrade Curl to version 8.7.0 or later

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ OpenSSL 1.1.1 < 1.1.1y Multiple Vulnerabilities (192965) ]

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

+Impact : Taking this action will resolve 2 different vulnerabilities (CVEs).


[ OpenSSL 3.0.0 < 3.0.14 Multiple Vulnerabilities (192966) ]

+ Action to take : Upgrade to OpenSSL version 3.0.14 or later.

+Impact : Taking this action will resolve 46 different vulnerabilities (CVEs).
```

```
[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : Jinja2
 vulnerability (USN-6787-1) (198044) ]

+ Action to take : Update the affected python-jinja2 and / or python3-jinja2 packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : LibTIFF
 vulnerability (USN-6827-1) (200307) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS. : less
 vulnerability (USN-6756-1) (194474) ]

+ Action to take : Update the affected less package.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : Vim vulnerability
 (USN-6698-1) (192219) ]

+ Action to take : Update the affected packages.


[ Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : klibc vulnerabilities
 (USN-6736-1) (193362) ]

+ Action to take : Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

+Impact : Taking this action will resolve 4 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 16.04 ESM / 18.04 ESM / 20.04 ESM / 22.04 ESM : Traceroute vulnerability (USN-6478-1)
 (185568) ]

+ Action to [...]
```

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
```

45405 - Reachable IPv6 address

Synopsis

The remote host may be reachable from the Internet.

Description

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

Solution

Disable IPv6 if you do not actually using it.

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

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/0

```

The following global addresss were gathered :

  - ['ipv6': fe80::290:bff:fea5:d295]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': fe80::290:bff:fea5:d28e]['scope': link]['scopeid': 0x20]['prefixlen': 64]
  - ['ipv6': ::1]['scope': host]['scopeid': 0x10]['prefixlen': 128]
  - ['ipv6': fe80::bede:49c7:42c5:8966]['scope': link]['scopeid': 0x20]['prefixlen': 64]
```

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: 2023/11/27

Plugin Output

tcp/22/ssh

```
  Process ID   : 552256
  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: 2023/11/27

Plugin Output

tcp/80/www

```

  Process ID   : 146583
  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: 2023/11/27

Plugin Output

udp/30041

```
  Process ID   : 195231
  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: 2023/11/27

Plugin Output

udp/30042

```
  Process ID   : 195582
  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: 2023/11/27

Plugin Output

tcp/30252

```
  Process ID   : 195215
  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: 2023/11/27

Plugin Output

tcp/42001/www

```
  Process ID   : 146583
  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: 2024/06/24

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: 2021/01/19

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: 2023/11/27

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: 2020/09/22

Plugin Output

tcp/22/ssh

```
SSH version : SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6
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 : Jul 02 11:32:07 2024 GMT

|-Subject   :
|-Not After : Jun 26 18:37:34 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
Jun 26 18:37:34 2024 GMT :

  Subject          : n/a
  Issuer           : CN=Caddy Local Authority - ECC Intermediate
  Not valid before : Jun 26 06:37:34 2024 GMT
  Not valid after  : Jun 26 18:37:34 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 AB 65 D3 9C E1 C0 39 BC 59 F5 29 77 F3 69 AB 9D

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:37:34 2024 GMT
Not Valid After: Jun 26 18:37:34 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 31 F7 74 6C 66 CB 87 8A F1 CD 96 94 3C 8F 73 EC AD C7 F3 B2
              9B AF 69 E4 5F A8 36 82 CD 37 B8 F4
Public Key Y: A6 E5 74 28 9C B5 86 3D 3B 9E 3B EA FF 05 C0 85 DF 00 02 5C
              B9 C8 BA 83 95 CC DC 8A A3 D0 86 73

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 EA 31 DD 45 C4 E2 C0 4E 25 D7 26 80 58 F1
           FF C3 4F 48 11 97 69 68 ED 95 49 5C 52 A9 C8 34 61 7E 02 20
           71 53 82 82 89 1D 91 2D 4F 7E A7 E0 72 12 F2 A8 2D FC 53 A9
           1B AA ED 2A 2C 52 B7 F3 C1 7E 56 FB
```

```
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: AA FA F3 20 9E 21 40 AF 07 23 08 4D DC BC C8 F5 85 95 97 83


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 43 BD 5B 51 83 A3 70 1C 8E 8F 01 A5 5C 6D 89 C4 5C 3E CB 27


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1


Fingerprints :

SHA-256 Fingerprint: 0D 2F EF 80 2C 04 EE FB D2 E6 CF 80 F3 FC E9 9A ED 9D 3D 1E
                     DD 62 85 BA 3B 2E 7F EB 89 88 DA EF
SHA-1 Fingerprint: DC AA 0B 20 C1 F6 F8 6D 50 E5 30 2A 59 68 1E 4A 83 05 DC D3
MD5 Fingerprint: 3E F2 21 39 3A F4 FF 59 AB 51 F3 4B DE 31 ED BC


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV+gAwIBAgIRAKtl05zhwDm8WfUpd/
Npq50wCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA2MjYwNjM3MzRa
 [...]
```

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 AB 65 D3 9C E1 C0 39 BC 59 F5 29 77 F3 69 AB 9D

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:37:34 2024 GMT
Not Valid After: Jun 26 18:37:34 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 31 F7 74 6C 66 CB 87 8A F1 CD 96 94 3C 8F 73 EC AD C7 F3 B2
              9B AF 69 E4 5F A8 36 82 CD 37 B8 F4
Public Key Y: A6 E5 74 28 9C B5 86 3D 3B 9E 3B EA FF 05 C0 85 DF 00 02 5C
```

```
              B9 C8 BA 83 95 CC DC 8A A3 D0 86 73

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 EA 31 DD 45 C4 E2 C0 4E 25 D7 26 80 58 F1
           FF C3 4F 48 11 97 69 68 ED 95 49 5C 52 A9 C8 34 61 7E 02 20
           71 53 82 82 89 1D 91 2D 4F 7E A7 E0 72 12 F2 A8 2D FC 53 A9
           1B AA ED 2A 2C 52 B7 F3 C1 7E 56 FB

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: AA FA F3 20 9E 21 40 AF 07 23 08 4D DC BC C8 F5 85 95 97 83


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 43 BD 5B 51 83 A3 70 1C 8E 8F 01 A5 5C 6D 89 C4 5C 3E CB 27


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV+gAwIBAgIRAKtl05zhwDm8WfUpd/
Npq50wCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA2MjYwNjM3MzRa
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFKr68yCeIUCvByMITdy8yPWFlZeDMB8GA1UdIwQYMBaAFEO9W1G
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 AB 65 D3 9C E1 C0 39 BC 59 F5 29 77 F3 69 AB 9D

Version: 3

Signature Algorithm: ECDSA With SHA-256

Not Valid Before: Jun 26 06:37:34 2024 GMT
Not Valid After: Jun 26 18:37:34 2024 GMT

Public Key Info:

Algorithm: EC Public Key
Elliptic Curve: P256
Key Length: 256 bits
Public Key X: 31 F7 74 6C 66 CB 87 8A F1 CD 96 94 3C 8F 73 EC AD C7 F3 B2
              9B AF 69 E4 5F A8 36 82 CD 37 B8 F4
Public Key Y: A6 E5 74 28 9C B5 86 3D 3B 9E 3B EA FF 05 C0 85 DF 00 02 5C
```

```
              B9 C8 BA 83 95 CC DC 8A A3 D0 86 73

Signature Length: 71 bytes / 568 bits
Signature: 00 30 45 02 21 00 EA 31 DD 45 C4 E2 C0 4E 25 D7 26 80 58 F1
           FF C3 4F 48 11 97 69 68 ED 95 49 5C 52 A9 C8 34 61 7E 02 20
           71 53 82 82 89 1D 91 2D 4F 7E A7 E0 72 12 F2 A8 2D FC 53 A9
           1B AA ED 2A 2C 52 B7 F3 C1 7E 56 FB

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: AA FA F3 20 9E 21 40 AF 07 23 08 4D DC BC C8 F5 85 95 97 83


Extension: Authority Key Identifier (2.5.29.35)
Critical: 0
Key Identifier: 43 BD 5B 51 83 A3 70 1C 8E 8F 01 A5 5C 6D 89 C4 5C 3E CB 27


Extension: Subject Alternative Name (2.5.29.17)
Critical: 1



PEM certificate :

-----BEGIN CERTIFICATE-----
MIIBuTCCAV+gAwIBAgIRAKtl05zhwDm8WfUpd/
Npq50wCgYIKoZIzj0EAwIwMzExMC8GA1UEAxMoQ2FkZHkgTG9jYWwgQXV0aG9yaXR5IC0gRUNDIEludGVybWVkaWF0ZTAeFw0yNDA2MjYwNjM3MzRa
wQEAwIHgDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFKr68yCeIUCvByMITdy8yPWFlZeDMB8GA1UdIwQYMBaAFEO9W1G
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/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.
```

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.
```

17975 - Service Detection (GET 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 an HTTP request.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/443/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  1.2.0  amd64  The installer of the Anapaya appliance.
  ii   anapaya-system-config  1.2.0  amd64  System configuration for Anapaya appliances.
  ii   apparmor  3.0.4-2ubuntu2.3  amd64  user-space parser utility for AppArmor
  ii   apt  2.4.11  amd64  commandline package manager
  ii   apt-transport-https  2.4.11  all  transitional package for https support
  ii   apt-utils  2.4.11  amd64  package management related utility programs
  ii   base-files  12ubuntu4.5  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  amd64  GNU Bourne Again SHell
  ii   bash-completion  1:2.11-5ubuntu1  all  programmable completion for the bash shell
  ii   bind9-dnsutils  1:9.18.18-0ubuntu0.22.04.2  amd64  Clients provided with BIND 9
  ii   bind9-host  1:9.18.18-0ubuntu0.22.04.2  amd64  DNS Lookup Utility
  ii   bind9-libs  1:9.18.18-0ubuntu0.22.04.2  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  amd64  extra utilities from 4.4BSD-Lite
  ii   bsdutils  1:2.37.2-4ubuntu3  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  2023031 [...]
```

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: 2024/04/24

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
```

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 following packages require a reboot :

systemd
```

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

```
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 192.168.112.1 :
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: 2024/06/24

Plugin Output

tcp/0

```
Nessus detected 22 installs of XZ Utils:

  Path    : /var/lib/docker/overlay2/
e2c734e730391f8c0232a402afd5d9ed2c3cc86247b5737a5130d7c5da3dd693/merged/bin/xz
  Version : unknown
  Path    : /var/lib/docker/
overlay2/78c25587e64b4df48912910324d9db53d2f6df585e6aa71467071cf20acdf688/diff/usr/lib/
liblzma.so.5.2.5
  Version : 5.2.5

  Path    : /var/lib/docker/
overlay2/0a0124157fa6efaf256d46f48211edf0593276aa6710f9e9c0268674f0d00086/diff/usr/lib/
liblzma.so.5.2.5
  Version : 5.2.5

  Path    : /var/lib/docker/
overlay2/6e67a7d3f82c0c57525de2addd80f62926577f41180822a04fc3b06326a577fa/diff/bin/xz
  Version : unknown

  Path    : /var/lib/docker/
overlay2/1c3a6bc1043c947a6318d1e1052a2657d38d8bc5eecbfead5dca5374dc7faca5/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.4
  Version : 5.2.4

  Path    : /var/lib/docker/
overlay2/487592c2b6545575ef3bb2e82f706b3211dc1793ae9cdefcee621da571807d08/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version : 5.2.5

  Path    : /var/lib/docker/
overlay2/1ec83b578c77fef6bba72f867d2532c82155d89a5f3047c51f435a81938932cf/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.4
  Version : 5.2.4

  Path    : /var/lib/docker/
overlay2/4575a4ca1b1d6cb833e9d1cb94b61094d86d4b000f4914c9236ac85aa4196bd4/diff/usr/bin/xz
  Version : 5.2.5

  Path    : /var/lib/docker/
overlay2/1eccf5fa4d23f4e56c1c190711d470fcdcf1ca38f99d3b8342a4c0b878ca50de/diff/usr/bin/xz
  Version : 5.2.4

  Path    : /var/lib/docker/overlay2/
ba1c04b0b739169856cf2bc9d31f2ae863fc51b62aa911747f39d0399f5d2882/diff/usr/lib/liblzma.so.5.2.9
  Version : 5.2.9

  Path    : /var/lib/docker/
overlay2/5bebb85d5d656eb7ac3812c25a40425e41cd4172ad92bdaf6eff8d5cdbc38512/diff/lib/x86_64-linux-gnu/
liblzma.so.5.2.5
  Version : 5.2.5

  Path    : /var/lib/docker/
overlay2/528b0bf74837aa7594b022dcaf26c51a11fedd15857268116aee9fcd07a33e8b/diff/bin/xz
  Version : unknown

  Path               : /usr/bin/xz
  Version            : 5.2.5
  Associated Package : xz-utils 5.2.5-2ubuntu1
  Managed by OS      : True

  Path    : /var/lib/docker/overlay2/e72cb6e4bfaf6f9eb83b47488b07ae9e8f588b9 [...]
```

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: 2024/05/31

Plugin Output

tcp/0

```
This machine is attached to an Ubuntu Pro subscription.
```

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  0.2  0.1 167232 11968 ?        Ss    2023 1069:38 /lib/systemd/systemd noquiet
 nosplash nofb --system --deserialize 43
root           2  0.0  0.0      0     0 ?        S     2023   0:03 [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  18:44 [ksoftirqd/0]
root          14  0.0  0.0      0     0 ?        I     2023 313:49 [rcu_sched]
root          15  0.0  0.0      0     0 ?        S     2023   0:53 [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   0:49 [migration/1]
root          22  0.0  0.0      0     0 ?        S     2023  12:06 [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   0:52 [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  : 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: 2024/06/24

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: 2024/06/24

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 7.81.0-1ubuntu1.15
  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 7.81.0-1ubuntu1.15
  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: 2024/06/24

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

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

control-64-2_0_2b.docker.container

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	0

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

control-64-2_0_2c.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

control-64-2_0_2d.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

daemon-64-2_0_2b.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

daemon-64-2_0_2c.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

daemon-64-2_0_2d.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

dataplane-control.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

dataplane.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

dispatcher.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

gateway.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

node-exporter.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

promtail.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

router.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities

telemetry.docker.container

0	0	0	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Host Information

IP:	192.168.112.1
MAC Address:	00:90:0B:A5:D2:91 00:90:0B:A5:D2:8F 02:42:1C:46:AA:4D 00:90:0B:A5:D2:93 00:90:0B:A5:D2:8E 00:90:0B:A5:D2:90 00:90:0B:A5:D2:92 00:90:0B:A5:D2:94 00:90:0B:A5:D2:95
OS:	Linux Kernel 5.15.0-79-generic on Ubuntu 22.04

Vulnerabilities