Scan Report

July 1, 2022

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Scan INFRA01". The scan started at Fri Jul 1 15:07:50 2022 UTC and ended at Fri Jul 1 15:11:11 2022 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.3.2	6	5	0	0	0
Total: 1	6	5	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 11 results selected by the filtering described above. Before filtering there were 77 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.3.2	SSH	Success	Protocol SSH, Port 22, User server

2 Results per Host

2.1 192.168.3.2

Host scan start	Fri Jul 1 15:08:21 2022 UTC
Host scan end	Fri Jul 1 15:11:03 2022 UTC

Service (Port)	Threat Level
general/tcp	High
general/tcp	Medium

2.1.1 High general/tcp

High (CVSS: 9.8) NVT: Debian: Security Advisory for ntfs-3g (DSA-5160-1)
. . . continues on next page . . .

... continued from previous page ...

Summary
The remote host is missing an update for the 'ntfs-3g' package(s) announced via the DSA-5160-1 advisory.

Vulnerability Detection Result
```
Vulnerable package: libntfs-3g883
Installed version:  2017.3.23AR.3-4+deb11u1
Fixed version:      1:2017.3.23AR.3-4+deb11u2
Vulnerable package: ntfs-3g
Installed version:  2017.3.23AR.3-4+deb11u1
Fixed version:      1:2017.3.23AR.3-4+deb11u2
```

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), these problems have been fixed in version 1:2017.3.23AR.3-3+deb10u2.
For the stable distribution (bullseye), these problems have been fixed in version 1:2017.3.23AR.3-4+deb11u2.
We recommend that you upgrade your ntfs-3g packages.

Affected Software/OS
'ntfs-3g' package(s) on Debian Linux.

Vulnerability Insight
Several vulnerabilities were discovered in NTFS-3G, a read-write NTFS driver for FUSE. A local user can take advantage of these flaws for local root privilege escalation.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory for ntfs-3g (DSA-5160-1)`
OID:1.3.6.1.4.1.25623.1.0.705160
Version used: `2022-06-14T14:05:23Z`

References
```
cve: CVE-2021-46790
cve: CVE-2022-30783
cve: CVE-2022-30784
cve: CVE-2022-30785
cve: CVE-2022-30786
cve: CVE-2022-30787
cve: CVE-2022-30788
cve: CVE-2022-30789
url: https://www.debian.org/security/2022/dsa-5160.html
url: https://security-tracker.debian.org/tracker/DSA-5160-1
advisory-id: DSA-5160-1
dfn-cert: DFN-CERT-2022-1218
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1217

High (CVSS: 9.8)
NVT: Debian: Security Advisory for dpkg (DSA-5147-1)

Summary
The remote host is missing an update for the 'dpkg' package(s) announced via the DSA-5147-1 advisory.

Vulnerability Detection Result
Vulnerable package: dpkg
Installed version: 1.20.9
Fixed version: 1.20.10
Vulnerable package: libdpkg-perl
Installed version: 1.20.9
Fixed version: 1.20.10

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), this problem has been fixed in version 1.19.8.
For the stable distribution (bullseye), this problem has been fixed in version 1.20.10.
We recommend that you upgrade your dpkg packages.

Affected Software/OS
'dpkg' package(s) on Debian Linux.

Vulnerability Insight
Max Justicz reported a directory traversal vulnerability in Dpkg::Source::Archive in dpkg, the Debian package management system. This affects extracting untrusted source packages in the v2 and v3 source package formats that include a debian.tar.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Debian: Security Advisory for dpkg (DSA-5147-1)
OID:1.3.6.1.4.1.25623.1.0.705147
Version used: 2022-06-09T03:04:58Z

References
cve: CVE-2022-1664
url: https://www.debian.org/security/2022/dsa-5147.html
url: https://security-tracker.debian.org/tracker/DSA-5147-1
advisory-id: DSA-5147-1
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1194

High (CVSS: 9.8)
NVT: Debian: Security Advisory for openssl (DSA-5139-1)

Summary
The remote host is missing an update for the 'openssl' package(s) announced via the DSA-5139-1 advisory.

Vulnerability Detection Result
```
Vulnerable package: libssl1.1
Installed version:  1.1.1n-0+deb11u1
Fixed version:      1.1.1n-0+deb11u2
Vulnerable package: openssl
Installed version:  1.1.1n-0+deb11u1
Fixed version:      1.1.1n-0+deb11u2
```

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), this problem has been fixed in version 1.1.1n-0+deb10u2.
For the stable distribution (bullseye), this problem has been fixed in version 1.1.1n-0+deb11u2.
We recommend that you upgrade your openssl packages.

Affected Software/OS
'openssl' package(s) on Debian Linux.

Vulnerability Insight
Elison Niven discovered that the c_rehash script included in OpenSSL did not sanitise shell meta characters which could result in the execution of arbitrary commands.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory for openssl (DSA-5139-1)`
OID:1.3.6.1.4.1.25623.1.0.705139
Version used: 2022-05-19T12:23:28Z

References
```
cve: CVE-2022-1292
url: https://www.debian.org/security/2022/dsa-5139.html
url: https://security-tracker.debian.org/tracker/DSA-5139-1
advisory-id: DSA-5139-1
cert-bund: CB-K22/0536
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1103
dfn-cert: DFN-CERT-2022-0986
```

High (CVSS: 9.8)
NVT: Debian: Security Advisory for openldap (DSA-5140-1)

Summary
The remote host is missing an update for the 'openldap' package(s) announced via the DSA-5140-1 advisory.

Vulnerability Detection Result
```
Vulnerable package: libldap-2.4-2
Installed version:  2.4.57+dfsg-3
Fixed version:      2.4.57+dfsg-3+deb11u1
Vulnerable package: libldap-common
Installed version:  2.4.57+dfsg-3
Fixed version:      2.4.57+dfsg-3+deb11u1
```

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), this problem has been fixed in version 2.4.47+dfsg-3+deb10u7.
For the stable distribution (bullseye), this problem has been fixed in version 2.4.57+dfsg-3+deb11u1.
We recommend that you upgrade your openldap packages.

Affected Software/OS
'openldap' package(s) on Debian Linux.

Vulnerability Insight
Jacek Konieczny discovered a SQL injection vulnerability in the back-sql backend to slapd in OpenLDAP, a free implementation of the Lightweight Directory Access Protocol, allowing an attacker to alter the database during an LDAP search operation when a specially crafted search filter is processed.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory for openldap (DSA-5140-1)`
OID:1.3.6.1.4.1.25623.1.0.705140
Version used: `2022-05-23T14:45:16Z`

References
```
cve: CVE-2022-29155
url: https://www.debian.org/security/2022/dsa-5140.html
url: https://security-tracker.debian.org/tracker/DSA-5140-1
advisory-id: DSA-5140-1
cert-bund: CB-K22/0541
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1107
```

High (CVSS: 8.1)
NVT: Debian: Security Advisory for rsyslog (DSA-5150-1)

Summary
The remote host is missing an update for the 'rsyslog' package(s) announced via the DSA-5150-1 advisory.

Vulnerability Detection Result
`Vulnerable package: rsyslog`
`Installed version: 8.2102.0-2`
`Fixed version: 8.2102.0-2+deb11u1`

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), this problem has been fixed in version 8.1901.0-1+deb10u2.
For the stable distribution (bullseye), this problem has been fixed in version 8.2102.0-2+deb11u1.
We recommend that you upgrade your rsyslog packages.

Affected Software/OS
'rsyslog' package(s) on Debian Linux.

Vulnerability Insight
Peter Agten discovered that several modules for TCP syslog reception in rsyslog, a system and kernel logging daemon, have buffer overflow flaws when octet-counted framing is used, which could result in denial of service or potentially the execution of arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory for rsyslog (DSA-5150-1)`
OID:1.3.6.1.4.1.25623.1.0.705150
Version used: `2022-05-31T14:07:25Z`

References
`cve: CVE-2022-24903`
`url: https://www.debian.org/security/2022/dsa-5150.html`
`url: https://security-tracker.debian.org/tracker/DSA-5150-1`
`advisory-id: DSA-5150-1`
`dfn-cert: DFN-CERT-2022-1267`
`dfn-cert: DFN-CERT-2022-1264`
`dfn-cert: DFN-CERT-2022-1167`
`dfn-cert: DFN-CERT-2022-1020`

High (CVSS: 7.5)
NVT: Debian: Security Advisory for webkit2gtk (DSA-5154-1)

... continues on next page ...

... continued from previous page ...

Summary
The remote host is missing an update for the 'webkit2gtk' package(s) announced via the DSA-5154-1 advisory.

Vulnerability Detection Result

```
Vulnerable package: gir1.2-javascriptcoregtk-4.0
Installed version:  2.36.0-3~deb11u1
Fixed version:      2.36.3-1~deb11u1
Vulnerable package: gir1.2-webkit2-4.0
Installed version:  2.36.0-3~deb11u1
Fixed version:      2.36.3-1~deb11u1
Vulnerable package: libjavascriptcoregtk-4.0-18
Installed version:  2.36.0-3~deb11u1
Fixed version:      2.36.3-1~deb11u1
Vulnerable package: libwebkit2gtk-4.0-37
Installed version:  2.36.0-3~deb11u1
Fixed version:      2.36.3-1~deb11u1
```

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), these problems have been fixed in version 2.36.3-1 deb10u1.
For the stable distribution (bullseye), these problems have been fixed in version 2.36.3-1 deb11u1.
We recommend that you upgrade your webkit2gtk packages.

Affected Software/OS
'webkit2gtk' package(s) on Debian Linux.

Vulnerability Insight
The following vulnerabilities have been discovered in the WebKitGTK web engine:
CVE-2022-26700 ryuzaki discovered that processing maliciously crafted web content may lead to code execution.
CVE-2022-26709 Chijin Zhou discovered that processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2022-26716 SorryMybad discovered that Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2022-26717 Jeonghoon Shin discovered that Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2022-26719 Dongzhuo Zhao discovered that Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2022-30293 Chijin Zhou discovered that processing maliciously crafted web content may lead to arbitrary code execution or to a denial of service (application crash).
CVE-2022-30294 Chijin Zhou discovered that processing maliciously crafted web content may lead to arbitrary code execution or to a denial of service (application crash).

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: Debian: Security Advisory for webkit2gtk (DSA-5154-1)
OID:1.3.6.1.4.1.25623.1.0.705154
Version used: 2022-06-15T03:04:08Z

References

cve: CVE-2022-26700
cve: CVE-2022-26709
cve: CVE-2022-26716
cve: CVE-2022-26717
cve: CVE-2022-26719
cve: CVE-2022-30293
cve: CVE-2022-30294
url: https://www.debian.org/security/2022/dsa-5154.html
url: https://security-tracker.debian.org/tracker/DSA-5154-1
advisory-id: DSA-5154-1
cert-bund: CB-K22/0627
cert-bund: CB-K22/0620
cert-bund: CB-K22/0619
cert-bund: CB-K22/0617
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1224
dfn-cert: DFN-CERT-2022-1136
dfn-cert: DFN-CERT-2022-1120
dfn-cert: DFN-CERT-2022-1117
dfn-cert: DFN-CERT-2022-1116

[return to 192.168.3.2]

2.1.2 Medium general/tcp

Medium (CVSS: 6.7)
NVT: Debian: Security Advisory for cups (DSA-5149-1)

Summary

The remote host is missing an update for the 'cups' package(s) announced via the DSA-5149-1 advisory.

Vulnerability Detection Result

Vulnerable package: cups
Installed version: 2.3.3op2-3+deb11u1
Fixed version: 2.3.3op2-3+deb11u2
Vulnerable package: cups-client
Installed version: 2.3.3op2-3+deb11u1
Fixed version: 2.3.3op2-3+deb11u2
Vulnerable package: cups-common

... continues on next page ...

... continued from previous page ...

```
Installed version:  2.3.3op2-3+deb11u1
Fixed version:      2.3.3op2-3+deb11u2
Vulnerable package: cups-core-drivers
Installed version:  2.3.3op2-3+deb11u1
Fixed version:      2.3.3op2-3+deb11u2
Vulnerable package: cups-daemon
Installed version:  2.3.3op2-3+deb11u1
Fixed version:      2.3.3op2-3+deb11u2
Vulnerable package: cups-ipp-utils
Installed version:  2.3.3op2-3+deb11u1
Fixed version:      2.3.3op2-3+deb11u2
Vulnerable package: cups-ppdc
Installed version:  2.3.3op2-3+deb11u1
Fixed version:      2.3.3op2-3+deb11u2
Vulnerable package: cups-server-common
Installed version:  2.3.3op2-3+deb11u1
Fixed version:      2.3.3op2-3+deb11u2
Vulnerable package: libcups2
Installed version:  2.3.3op2-3+deb11u1
Fixed version:      2.3.3op2-3+deb11u2
```

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), this problem has been fixed in version 2.2.10-6+deb10u6.
For the stable distribution (bullseye), this problem has been fixed in version 2.3.3op2-3+deb11u2.
We recommend that you upgrade your cups packages.

Affected Software/OS
'cups' package(s) on Debian Linux.

Vulnerability Insight
Joshua Mason discovered that a logic error in the validation of the secret key used in the local authorisation mode of the CUPS printing system may result in privilege escalation.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory for cups (DSA-5149-1)`
OID:1.3.6.1.4.1.25623.1.0.705149
Version used: `2022-06-09T03:04:58Z`

References

```
cve: CVE-2022-26691
url: https://www.debian.org/security/2022/dsa-5149.html
url: https://security-tracker.debian.org/tracker/DSA-5149-1
advisory-id: DSA-5149-1
cert-bund: CB-K22/0654
```

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1234
dfn-cert: DFN-CERT-2022-1197

Medium (CVSS: 6.5)
NVT: Debian: Security Advisory for libxml2 (DSA-5142-1)

Summary
The remote host is missing an update for the 'libxml2' package(s) announced via the DSA-5142-1 advisory.

Vulnerability Detection Result
Vulnerable package: libxml2
Installed version: 2.9.10+dfsg-6.7+deb11u1
Fixed version: 2.9.10+dfsg-6.7+deb11u2

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), this problem has been fixed in version 2.9.4+dfsg1-7+deb10u4.
For the stable distribution (bullseye), this problem has been fixed in version 2.9.10+dfsg-6.7+deb11u2.
We recommend that you upgrade your libxml2 packages.

Affected Software/OS
'libxml2' package(s) on Debian Linux.

Vulnerability Insight
Felix Wilhelm reported that several buffer handling functions in libxml2, a library providing support to read, modify and write XML and HTML files, don't check for integer overflows, resulting in out-of-bounds memory writes if specially crafted, multi-gigabyte XML files are processed. An attacker can take advantage of this flaw for denial of service or execution of arbitrary code.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Debian: Security Advisory for libxml2 (DSA-5142-1)
OID:1.3.6.1.4.1.25623.1.0.705142
Version used: 2022-05-24T14:04:10Z

References
cve: CVE-2022-29824
url: https://www.debian.org/security/2022/dsa-5142.html
url: https://security-tracker.debian.org/tracker/DSA-5142-1
advisory-id: DSA-5142-1
cert-bund: CB-K22/0531

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1183
dfn-cert: DFN-CERT-2022-1152
dfn-cert: DFN-CERT-2022-1112
dfn-cert: DFN-CERT-2022-0981

Medium (CVSS: 5.0)
NVT: Debian: Security Advisory for firefox-esr (DSA-5156-1)

Summary
The remote host is missing an update for the 'firefox-esr' package(s) announced via the DSA-5156-1 advisory.

Vulnerability Detection Result
Vulnerable package: firefox-esr
Installed version: 91.8.0esr-1~deb11u1
Fixed version: 91.10.0esr-1~deb11u1
Vulnerable package: firefox-esr-l10n-fr
Installed version: 91.8.0esr-1~deb11u1
Fixed version: 91.10.0esr-1~deb11u1

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), these problems have been fixed in version 91.10.0esr-1 deb10u1.
For the stable distribution (bullseye), these problems have been fixed in version 91.10.0esr-1 deb11u1.
We recommend that you upgrade your firefox-esr packages.

Affected Software/OS
'firefox-esr' package(s) on Debian Linux.

Vulnerability Insight
Multiple security issues have been found in the Mozilla Firefox web browser, which could potentially result in the execution of arbitrary code, information disclosure or spoofing.

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: Debian: Security Advisory for firefox-esr (DSA-5156-1)
OID:1.3.6.1.4.1.25623.1.0.705156
Version used: 2022-06-09T12:37:46Z

References
cve: CVE-2022-31736
cve: CVE-2022-31737

... continues on next page ...

... continued from previous page ...

cve: CVE-2022-31738
cve: CVE-2022-31740
cve: CVE-2022-31741
cve: CVE-2022-31742
cve: CVE-2022-31747
url: https://www.debian.org/security/2022/dsa-5156.html
url: https://security-tracker.debian.org/tracker/DSA-5156-1
advisory-id: DSA-5156-1
cert-bund: CB-K22/0671
dfn-cert: DFN-CERT-2022-1303
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1231
dfn-cert: DFN-CERT-2022-1230

Medium (CVSS: 5.0)
NVT: Debian: Security Advisory for firefox-esr (DSA-5143-1)

Summary
The remote host is missing an update for the 'firefox-esr' package(s) announced via the DSA-5143-1 advisory.

Vulnerability Detection Result
Vulnerable package: firefox-esr
Installed version: 91.8.0esr-1~deb11u1
Fixed version: 91.9.1esr-1~deb11u1
Vulnerable package: firefox-esr-l10n-fr
Installed version: 91.8.0esr-1~deb11u1
Fixed version: 91.9.1esr-1~deb11u1

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), these problems have been fixed in version 91.9.1esr-1 deb10u1.
For the stable distribution (bullseye), these problems have been fixed in version 91.9.1esr-1 deb11u1.
We recommend that you upgrade your firefox-esr packages.

Affected Software/OS
'firefox-esr' package(s) on Debian Linux.

Vulnerability Insight
Manfred Paul discovered two security issues in the Mozilla Firefox web browser, which could result in the execution of arbitrary code.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory for firefox-esr (DSA-5143-1)`
OID:1.3.6.1.4.1.25623.1.0.705143
Version used: `2022-05-24T01:00:52Z`

References

```
cve: CVE-2022-1529
cve: CVE-2022-1802
url: https://www.debian.org/security/2022/dsa-5143.html
url: https://security-tracker.debian.org/tracker/DSA-5143-1
advisory-id: DSA-5143-1
cert-bund: CB-K22/0642
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1173
dfn-cert: DFN-CERT-2022-1162
```

Medium (CVSS: 5.0)
NVT: Debian: Security Advisory for firefox-esr (DSA-5129-1)

Summary
The remote host is missing an update for the 'firefox-esr' package(s) announced via the DSA-5129-1 advisory.

Vulnerability Detection Result

```
Vulnerable package: firefox-esr
Installed version:  91.8.0esr-1~deb11u1
Fixed version:      91.9.0esr-1~deb11u1
Vulnerable package: firefox-esr-l10n-fr
Installed version:  91.8.0esr-1~deb11u1
Fixed version:      91.9.0esr-1~deb11u1
```

Solution:
Solution type: VendorFix
For the oldstable distribution (buster), these problems have been fixed in version 91.9.0esr-1 deb10u1.
For the stable distribution (bullseye), these problems have been fixed in version 91.9.0esr-1 deb11u1.
We recommend that you upgrade your firefox-esr packages.

Affected Software/OS
'firefox-esr' package(s) on Debian Linux.

Vulnerability Insight
Multiple security issues have been found in the Mozilla Firefox web browser, which could potentially result in the execution of arbitrary code, information disclosure or spoofing.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Checks if a vulnerable package version is present on the target host.
Details: `Debian: Security Advisory for firefox-esr (DSA-5129-1)`
OID:1.3.6.1.4.1.25623.1.0.705129
Version used: `2022-05-06T01:00:24Z`

References
`cve: CVE-2022-29909`
`cve: CVE-2022-29911`
`cve: CVE-2022-29912`
`cve: CVE-2022-29914`
`cve: CVE-2022-29916`
`cve: CVE-2022-29917`
`url: https://www.debian.org/security/2022/dsa-5129.html`
`url: https://security-tracker.debian.org/tracker/DSA-5129-1`
`advisory-id: DSA-5129-1`
`cert-bund: CB-K22/0542`
`cert-bund: CB-K22/0534`
`dfn-cert: DFN-CERT-2022-1267`
`dfn-cert: DFN-CERT-2022-1173`
`dfn-cert: DFN-CERT-2022-1007`
`dfn-cert: DFN-CERT-2022-1003`
`dfn-cert: DFN-CERT-2022-0991`
`dfn-cert: DFN-CERT-2022-0978`

[return to 192.168.3.2]