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 L01". The scan started at Sat Jun 18 04:41:49 2022 UTC and ended at Sat Jun 18 04:45:45 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
192.168.2.222	0	2	0	0	0
Total: 1	0	2	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 2 results selected by the filtering described above. Before filtering there were 146 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.2.222	SSH	Success	Protocol SSH, Port 22, User l01

2 Results per Host

2.1 192.168.2.222

Host scan start	Sat Jun 18 04:42:10 2022 UTC
Host scan end	Sat Jun 18 04:45:42 2022 UTC

Service (Port)	Threat Level
general/tcp	Medium

2.1.1 Medium general/tcp

Medium (CVSS: 5.0)
NVT: Google Chrome Security Updates(stable-channel-update-for-desktop_24-2022-05)-Linux

Product detection result

. . . continues on next page . . .

... continued from previous page ...

cpe:/a:google:chrome:101.0.4951.54
Detected by Google Chrome Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.256
↪23.1.0.801446)

Summary
Google Chrome is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 101.0.4951.54
Fixed version: 102.0.5005.61
Installation
path / port: /usr/bin/google-chrome

Impact
Successful exploitation will allow attackers to conduct out-of-bounds memory access, execute arbitrary code, disclose sensitive information and cause a denial of service condition.

Solution:
Solution type: VendorFix
Upgrade to Google Chrome version 102.0.5005.61 or later. Please see the references for more information.

Affected Software/OS
Google Chrome version prior to 102.0.5005.61 on Linux

Vulnerability Insight
Multiple flaws exist due to,
- Multiple use after free errors in Indexed DB, ANGLE, Messaging, User Education, etc.
- Insufficient policy enforcement in File System API.
- Out of bounds read in DevTools.
- Inappropriate implementation in Extensions.
- Insufficient validation of untrusted input in Data Transfer.
- Type Confusion in V8.
- Multiple insufficient policy enforcement errors in Extensions API, COOP, and Safe Browsing.
- Inappropriate implementation in PDF.
- Heap buffer overflow in DevTools.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Google Chrome Security Updates(stable-channel-update-for-desktop_24-2022-05)-Li.
↪..
OID:1.3.6.1.4.1.25623.1.0.821255
Version used: 2022-06-01T13:00:54Z

Product Detection Result

... continues on next page ...

... continued from previous page ...

Product: cpe:/a:google:chrome:101.0.4951.54
Method: Google Chrome Detection (Linux/Unix SSH Login)
OID: 1.3.6.1.4.1.25623.1.0.801446)

References

cve: CVE-2022-1853
cve: CVE-2022-1854
cve: CVE-2022-1855
cve: CVE-2022-1856
cve: CVE-2022-1857
cve: CVE-2022-1858
cve: CVE-2022-1859
cve: CVE-2022-1860
cve: CVE-2022-1861
cve: CVE-2022-1862
cve: CVE-2022-1863
cve: CVE-2022-1864
cve: CVE-2022-1865
cve: CVE-2022-1866
cve: CVE-2022-1867
cve: CVE-2022-1868
cve: CVE-2022-1869
cve: CVE-2022-1870
cve: CVE-2022-1871
cve: CVE-2022-1872
cve: CVE-2022-1873
cve: CVE-2022-1874
cve: CVE-2022-1875
cve: CVE-2022-1876
url: https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-des
↪ktop_24.html
cert-bund: CB-K22/0669
cert-bund: CB-K22/0649
dfn-cert: DFN-CERT-2022-1302
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1233
dfn-cert: DFN-CERT-2022-1184

Medium (CVSS: 5.0)
NVT: Google Chrome Security Update(stable-channel-update-for-desktop_10-2022-05) - Linux

Product detection result

cpe:/a:google:chrome:101.0.4951.54
Detected by Google Chrome Detection (Linux/Unix SSH Login) (OID: 1.3.6.1.4.1.256
↪23.1.0.801446)

... continues on next page ...

... continued from previous page ...

Summary
Google Chrome is prone to multiple vulnerabilities.

Vulnerability Detection Result
Installed version: 101.0.4951.54
Fixed version: 101.0.4951.64
Installation
path / port: /usr/bin/google-chrome

Impact
Successful exploitation will allow attackers to conduct execute arbitrary code, disclose sensitive information and cause denial of service condition.

Solution:
Solution type: VendorFix
Upgrade to Google Chrome version 101.0.4951.64 or later. Please see the references for more information.

Affected Software/OS
Google Chrome version prior to 101.0.4951.64 on Linux

Vulnerability Insight
Multiple flaws are due to,
- Multiple use after free errors.
- Anappropriate implementation in Web Contents.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: Google Chrome Security Update(stable-channel-update-for-desktop_10-2022-05) - L.
↪..
OID:1.3.6.1.4.1.25623.1.0.821244
Version used: 2022-05-19T11:50:09Z

Product Detection Result
Product: cpe:/a:google:chrome:101.0.4951.54
Method: Google Chrome Detection (Linux/Unix SSH Login)
OID: 1.3.6.1.4.1.25623.1.0.801446)

References
cve: CVE-2022-1633
cve: CVE-2022-1634
cve: CVE-2022-1635
cve: CVE-2022-1636

... continues on next page ...

... continued from previous page ...

```
cve: CVE-2022-1637
cve: CVE-2022-1638
cve: CVE-2022-1639
cve: CVE-2022-1640
cve: CVE-2022-1641
url: https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-des
↪ktop_10.html
cert-bund: CB-K22/0582
dfn-cert: DFN-CERT-2022-1267
dfn-cert: DFN-CERT-2022-1026
```

[return to 192.168.2.222]
