

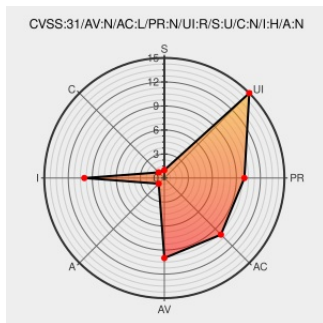


# CVE-2020-6562

Published on: 09/21/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

## CVE-2020-6562

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Insufficient policy enforcement in Blink in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.

CVE-2020-6562 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Google - Chrome** version < 85.0.4183.83

CVSS3 Score: **6.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description                                                             | Tags                                                                 | Link                                       |
|-------------------------------------------------------------------------|----------------------------------------------------------------------|--------------------------------------------|
| [security-announce] openSUSE-SU-2020:1514-1: important: Security update | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a> | <a href="#">SUSE openSUSE-SU-2020:1514</a> |

|                                                                                                     |                                                                                                                                              |                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| important: Security update                                                                          | <a href="#">Third Party Advisory</a><br><a href="#">lists.opensuse.org</a><br><a href="#">text/html</a>                                      |                                                                                                                                                                                          |
| [security-announce] openSUSE-SU-2020:1510-1:<br>important: Security update                          | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">lists.opensuse.org</a><br><a href="#">text/html</a>      |  <a href="#">SUSE openSUSE-SU-2020:1510</a>                                                           |
| [SECURITY] Fedora 33 Update: chromium-85.0.4183.83-1.fc33 - package-announce - Fedora Mailing-Lists | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">lists.fedoraproject.org</a><br><a href="#">text/html</a> |  <a href="#">FEDORA FEDORA-2020-6da740d38c</a>                                                        |
| Debian -- Security Information -- DSA-4824-1 chromium                                               | <a href="#">Third Party Advisory</a><br><a href="#">www.debian.org</a><br><a href="#">Deprecated Link</a><br><a href="#">text/html</a>       |  <a href="#">DEBIAN DSA-4824</a>                                                                      |
| Chrome Releases: Stable Channel Update for Desktop                                                  | <a href="#">Vendor Advisory</a><br><a href="#">chromereleases.googleblog.com</a><br><a href="#">text/html</a>                                |  <a href="#">MISC chromereleases.googleblog.com/2020/08/stable-channel-update-for-desktop_25.html</a> |
| Qt WebEngine: Multiple vulnerabilities (GLSA 202101-30) — Gentoo security                           | <a href="#">Third Party Advisory</a><br><a href="#">security.gentoo.org</a><br><a href="#">text/html</a>                                     |  <a href="#">GENTOO GLSA-202101-30</a>                                                                |
| [security-announce] openSUSE-SU-2020:1499-1:<br>important: Security update                          | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">lists.opensuse.org</a><br><a href="#">text/html</a>      |  <a href="#">SUSE openSUSE-SU-2020:1499</a>                                                           |
| 1086845 - chromium - An open-source project to help move the web forward. - Monorail                | <a href="#">Third Party Advisory</a><br><a href="#">crlbug.com</a><br><a href="#">text/html</a>                                              |  <a href="#">MISC crbug.com/1086845</a>                                                             |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

## Related QID Numbers

[690503](#) Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (d73bc4e6-e7c4-11ea-a878-e09467587c17)

## Known Affected Configurations (CPE V2.3)

| Type             | Vendor                        | Product                      | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 33      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 33      | All    | All     | All      |
| Application      | <a href="#">Google</a>        | <a href="#">Chrome</a>       | All     | All    | All     | All      |
| Application      | <a href="#">Google</a>        | <a href="#">Chrome</a>       | All     | All    | All     | All      |

|                                                  |          |               |      |     |     |     |
|--------------------------------------------------|----------|---------------|------|-----|-----|-----|
| Application                                      | Opensuse | Backports Sle | 15.0 | sp1 | All | All |
| Application                                      | Opensuse | Backports Sle | 15.0 | sp2 | All | All |
| Application                                      | Opensuse | Backports Sle | 15.0 | sp1 | All | All |
| Application                                      | Opensuse | Backports Sle | 15.0 | sp2 | All | All |
| Operating System                                 | Opensuse | Leap          | 15.1 | All | All | All |
| Operating System                                 | Opensuse | Leap          | 15.2 | All | All | All |
| Operating System                                 | Opensuse | Leap          | 15.1 | All | All | All |
| Operating System                                 | Opensuse | Leap          | 15.2 | All | All | All |
| cpe:2.3:o:debian:debian_linux:10.0:*****:        |          |               |      |     |     |     |
| cpe:2.3:o:debian:debian_linux:10.0:*****:        |          |               |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:33:*****:         |          |               |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:33:*****:         |          |               |      |     |     |     |
| cpe:2.3:a:google:chrome:*****:                   |          |               |      |     |     |     |
| cpe:2.3:a:google:chrome:*****:                   |          |               |      |     |     |     |
| cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*****: |          |               |      |     |     |     |
| cpe:2.3:a:opensuse:backports_sle:15.0:sp2:*****: |          |               |      |     |     |     |
| cpe:2.3:a:opensuse:backports_sle:15.0:sp1:*****: |          |               |      |     |     |     |
| cpe:2.3:a:opensuse:backports_sle:15.0:sp2:*****: |          |               |      |     |     |     |
| cpe:2.3:o:opensuse:leap:15.1:*****:              |          |               |      |     |     |     |
| cpe:2.3:o:opensuse:leap:15.2:*****:              |          |               |      |     |     |     |
| cpe:2.3:o:opensuse:leap:15.1:*****:              |          |               |      |     |     |     |
| cpe:2.3:o:opensuse:leap:15.2:*****:              |          |               |      |     |     |     |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)