

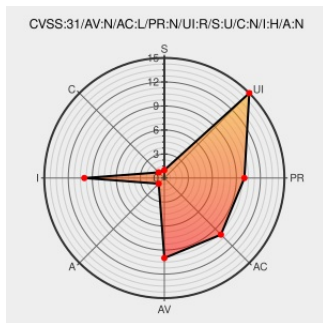


# CVE-2020-6475

Published on: 05/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:05 PM UTC

## CVE-2020-6475

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

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

Incorrect implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.

CVE-2020-6475 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Google - Chrome** version < 83.0.4103.61

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                                  |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------|
| Chromium, Google Chrome: Multiple vulnerabilities (GI SA 202006-02) — Gentoo security | <a href="#">Third Party Advisory</a><br><a href="#">security.gentoo.org</a> | <a href="#">GENTOO GLSA-202006-02</a> |

|                                                                                                      |                                                                                                                                                         |                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [SECURITY] Fedora 31 Update: chromium-83.0.4103.116-3.fc31 - package-announce - Fedora Mailing-Lists | <a href="#">security.gentoo.org</a><br><a href="#">text/html</a>                                                                                        |                                                                                                                                                                                                             |
| [SECURITY] Fedora 31 Update: chromium-83.0.4103.116-3.fc31 - package-announce - Fedora Mailing-Lists | <a href="#">Third Party Advisory</a><br><a href="#">lists.fedoraproject.org</a><br><a href="#">text/html</a>                                            |  <a href="#">FEDORA FEDORA-2020-77f89ab772</a>                                                                           |
| Debian -- Security Information -- DSA-4714-1 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-4714</a>                                                                                         |
| [security-announce] openSUSE-SU-2020:0823-1: 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-2020:0823</a>                                                                              |
| Chrome Releases: Stable Channel Update for Desktop                                                   | <a href="#">Release Notes</a><br><a href="#">Vendor Advisory</a><br><a href="#">chromereleases.googleblog.com</a><br><a href="#">text/html</a>          |  <a href="#">MISC</a><br><a href="#">chromereleases.googleblog.com/2020/05/stable-channel-update-for-desktop_19.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] Fedora 32 Update: chromium-83.0.4103.116-3.fc32 - package-announce - Fedora Mailing-Lists | <a href="#">Third Party Advisory</a><br><a href="#">lists.fedoraproject.org</a><br><a href="#">text/html</a>                                            |  <a href="#">FEDORA FEDORA-2020-08561721ad</a>                                                                           |
| 1020026 - chromium - An open-source project to help move the web forward. - Monorail                 | <a href="#">Exploit</a><br><a href="#">Issue Tracking</a><br><a href="#">Vendor Advisory</a><br><a href="#">crlbug.com</a><br><a href="#">text/html</a> |  <a href="#">MISC crlbug.com/1020026</a>                                                                                |
| [security-announce] openSUSE-SU-2020:0832-1: 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-2020:0832</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).

There are currently no QIDs associated with this CVE

#### 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> | 9.0     | All    | All     | All      |
| 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> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Fedora</a> | <a href="#">Fedora Linux</a> | 31      | All    | All     | All      |

|                                                  |                               |                               |      |     |     |     |
|--------------------------------------------------|-------------------------------|-------------------------------|------|-----|-----|-----|
| Operating System                                 | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>        | 31   | All | All | All |
| Operating System                                 | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>        | 32   | All | All | All |
| Operating System                                 | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>        | 31   | All | All | All |
| Operating System                                 | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>        | 32   | 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                                      | <a href="#">Opensuse</a>      | <a href="#">Backports Sle</a> | 15.0 | sp1 | All | All |
| Application                                      | <a href="#">Opensuse</a>      | <a href="#">Backports Sle</a> | 15.0 | sp1 | All | All |
| Operating System                                 | <a href="#">Opensuse</a>      | <a href="#">Leap</a>          | 15.1 | All | All | All |
| Operating System                                 | <a href="#">Opensuse</a>      | <a href="#">Leap</a>          | 15.1 | All | All | All |
| cpe:2.3:o:debian:debian_linux:10.0:*****:        |                               |                               |      |     |     |     |
| cpe:2.3:o:debian:debian_linux:9.0:*****:         |                               |                               |      |     |     |     |
| cpe:2.3:o:debian:debian_linux:10.0:*****:        |                               |                               |      |     |     |     |
| cpe:2.3:o:debian:debian_linux:9.0:*****:         |                               |                               |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:31:*****:         |                               |                               |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:32:*****:         |                               |                               |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:31:*****:         |                               |                               |      |     |     |     |
| cpe:2.3:o:fedoraproject:fedora:32:*****:         |                               |                               |      |     |     |     |
| 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:sp1:*****: |                               |                               |      |     |     |     |
| cpe:2.3:o:opensuse:leap:15.1:*****:              |                               |                               |      |     |     |     |
| cpe:2.3:o:opensuse:leap:15.1:*****:              |                               |                               |      |     |     |     |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)