



# CVE-2019-13730

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2019-13730   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | chrome-cve-admin@google.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2019-12-10 22:15:00 UTC  |
| <b>Updated</b>         | 2023-11-07 03:04:00 UTC  |
| <b>Description</b>     | Type confusion in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap overflow |

## Risk And Classification

**Problem Types:** CWE-787 | CWE-843

## NVD Known Affected Configurations (CPE 2.3)

| 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="#">Fedoraproject</a> | <a href="#">Fedora</a>                                     | 30      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>                                     | 31      | 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="#">Novell</a>        | <a href="#">Suse Package Hub For Suse Linux Enterprise</a> | 12      | All    | All     | All      |
| Operating System | <a href="#">Opensuse</a>      | <a href="#">Backports</a>                                  | sle-15  | sp1    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux Desktop</a>                   | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux For Scientific Computing</a>  | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux Server</a>                    | 6.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>        | <a href="#">Enterprise Linux Workstation</a>               | 6.0     | All    | All     | All      |

## References

| Reference  | Source | Link  |
|--|--------|---|
| Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202003-08) — Gentoo security | GENTOO | <a href="https://security.gentoo.org">security.gentoo.org</a> |
| Red Hat Customer Portal  | REDHAT | <a href="https://access.redhat.com">access.redhat.com</a>     |

|  |         |  |
|--|---------|--|
| 1028862 - chromium - An open-source project to help move the web forward. - Monorail                 | MISC    | <a href="http://crbug.com">crbug.com</a>                             |
| [security-announce] openSUSE-SU-2019:2692-1: important: Security update                              | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>           |
| Debian -- Security Information -- DSA-4606-1 chromium  | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>                   |
| Bugtraq: [SECURITY] [DSA 4606-1] chromium security update  | BUGTRAQ | <a href="http://seclists.org">seclists.org</a>                       |
| [SECURITY] Fedora 30 Update: chromium-79.0.3945.117-1.fc30 - package-announce - Fedora Mailing-Lists |         | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| [SECURITY] Fedora 31 Update: chromium-79.0.3945.79-1.fc31 - package-announce - Fedora Mailing-Lists  | FEDORA  | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| Chrome Releases: Stable Channel Update for Desktop   | MISC    | <a href="http://chromereleases.com">chromereleases.com</a>           |
| [security-announce] openSUSE-SU-2019:2694-1: important: Security update                              | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>           |
| [SECURITY] Fedora 31 Update: chromium-79.0.3945.79-1.fc31 - package-announce - Fedora Mailing-Lists  |         | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| [SECURITY] Fedora 30 Update: chromium-79.0.3945.117-1.fc30 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |
| CVE Program record   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                         |
| NVD vulnerability detail   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                       |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**