



# CVE-2019-5871

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

## Summary

<b>CVE</b>	CVE-2019-5871
<b>State</b>	PUBLIC
<b>Assigner</b>	security@google.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-11-25 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:12:00 UTC
<b>Description</b>	Heap buffer overflow in Skia in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap c

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

## References

Reference	Source	Link	Tag
Chrome Releases: Stable Channel Update for Desktop	MISC	<a href="https://chromereleases.googleblog.com">chromereleases.googleblog.com</a>	Ven
990570 - chromium - An open-source project to help move the web forward. - Monorail		<a href="https://crbug.com">crbug.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710117](#) Gentoo Linux Chromium, Google Chrome Multiple vulnerabilities (GLSA 201911-06)

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](#).

**Free CVE JSON API** [cve.report/api](#)

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