



# CVE-2021-21197

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

## Summary

<b>CVE</b>	CVE-2021-21197
<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>	2021-04-09 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:29:00 UTC
<b>Description</b>	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit h

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	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>	34	All	All	All
Application	<a href="#">Google</a>	<a href="#">Chrome</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 34 Update: chromium-90.0.4430.93-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Chrome Releases: Stable Channel Update for Desktop	MISC	<a href="#">chromereleases.googleusercontent.com</a>
Chromium, Google Chrome: Multiple vulnerabilities (GLSA 202104-08) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
[SECURITY] Fedora 32 Update: chromium-90.0.4430.93-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: chromium-90.0.4430.93-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: chromium-90.0.4430.93-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 32 Update: chromium-90.0.4430.93-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>
1173903 - chromium - An open-source project to help move the web forward. - Monorail	MISC	<a href="#">crbug.com</a>
[SECURITY] Fedora 33 Update: chromium-90.0.4430.93-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

178528	Debian Security Update for chromium (DSA 4886-1)
179696	Debian Security Update for chromium (CVE-2021-21197)
281203	Fedora Security Update for chromium (FEDORA-2021-35d2bb4627)
281204	Fedora Security Update for chromium (FEDORA-2021-ff893e12c5)
281205	Fedora Security Update for chromium (FEDORA-2021-c3754414e7)
375426	Google Chrome Prior To 89.0.4389.114 Multiple Vulnerabilities
375456	Microsoft Edge Based On Chromium Prior to 89.0.774.68 Multiple Vulnerabilities
501812	Alpine Linux Security Update for chromium
504607	Alpine Linux Security Update for chromium
690189	Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (bddadaa4-9227-11eb-99c5-e09467587c17)
710018	Gentoo Linux Chromium, Google Chrome Multiple Vulnerabilities (GLSA 202104-08)
750256	OpenSUSE Security Update for opera (openSUSE-SU-2021:0592-1)
750282	OpenSUSE Security Update for chromium (openSUSE-SU-2021:0513-1)

© [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](#) 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](#)