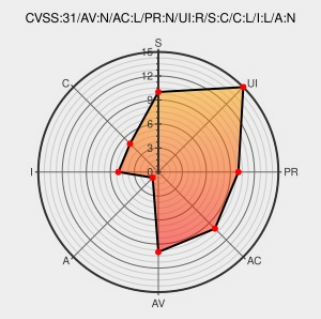
CVE-2021-37999

Published on: 11/23/2021 12:00:00 AM UTC

Last Modified on: 01/15/2022 03:15:00 PM UTC

CVE-2021-37999

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Chrome from Google contain the following vulnerability:

Insufficient data validation in New Tab Page in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to inject arbitrary scripts or HTML in a new browser tab via a crafted HTML page.

CVE-2021-37999 has been assigned by chrome-cve-admin@google.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Google** - **Chrome** version **< 95.0.4638.69**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-5046-1 chromium	www.debian.org Depreciated Link	DEBIAN DSA-5046

	text/html	
1251541 - chromium - An open-source project to help move the web forward. - Monorail	crbug.com text/html	MISC crbug.com/1251541
[SECURITY] Fedora 34 Update: chromium-96.0.4664.110-3.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-6a292e2cf4
Chrome Releases: Stable Channel Update for Desktop	chromereleases.googleblog.com text/html	MISC chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_28.html

Related QID Numbers

179000 Debian Security Update for chromium (DSA 5046-1)

282220 Fedora Security Update for chromium (FEDORA-2021-6a292e2cf4)

376000 Google Chrome Prior to 95.0.4638.69 Multiple Vulnerabilities

376010 Microsoft Edge Based on Chromium Prior to 95.0.1020.40 Multiple Vulnerabilities

690221 Free Berkeley Software Distribution (FreeBSD) Security Update for chromium (976d7bf9-38ea-11ec-b3b0-3065ec8fd3ec)

751335 OpenSUSE Security Update for chromium (openSUSE-SU-2021:1462-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Chrome	All	All	All	All

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@ashketchum_16	I have discovered new CVE-2021-37999 in @googlechrome affecting Linux, Windows, Chrome, Mac, Fuchsia and Lacros Ope… twitter.com/i/web/status/1…	2021-11-01 18:07:33
@ipssignatures	The vuln CVE-2021-37999 has a tweet created 0 days ago and retweeted 11 times. twitter.com/ashketchum_16/… #pow1rtrtwwcve	2021-11-02 10:06:01
@1337in	[Chrome] XSS in New-Tab Page [CVE-2021-37999] The Chrome New Tab Page was vulnerable to a stored cross-site script… twitter.com/i/web/status/1…	2021-11-12 09:58:16
@CVEreport	CVE-2021-37999 : Insufficient data validation in New Tab Page in Google Chrome prior to 95.0.4638.69 allowed a remo… twitter.com/i/web/status/1…	2021-11-23 21:33:34
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution	2021-11-01 13:16:00

← Previous ID

Next ID→