CVE-2021-30560

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-30560
State	PUBLIC
Assigner	chrome-cve-admin@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-03 19:15:00 UTC
Updated	2024-03-27 14:45:00 UTC
Description	Use after free in Blink XSLT in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Splunk	Universal Forwarder	All	All	All	All
Application	Splunk	Universal Forwarder	9.1.0	All	All	All
Application	Xmlsoft	Libxslt	All	All	All	All

References

Reference	Source	Link	Ta
Chrome Releases: Stable Channel Update for Desktop	MISC	chromereleases.googleblog.com	
Debian -- Security Information -- DSA-5216-1 libxslt	DEBIAN	www.debian.org	
[SECURITY] [DLA 3101-1] libxslt security update	MLIST	lists.debian.org	
libxslt: Multiple Vulnerabilities (GLSA 202310-23) — Gentoo security	GENTOO	security.gentoo.org	
1219209 - chromium - An open-source project to help move the web forward. - Monorail	MISC	crbug.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180585 Debian Security Update for chromium (CVE-2021-30560)

180960 Debian Security Update for libxslt (DSA 5216-1)

181001 Debian Security Update for libxslt (DLA 3101-1)

198907 Ubuntu Security Notification for Libxslt Vulnerabilities (USN-5575-1)

281721 Fedora Security Update for chromium (FEDORA-2021-9f62d36f09)

281741 Fedora Security Update for chromium (FEDORA-2021-30c84b4924)

282329 Fedora Security Update for qt5 (FEDORA-2022-e39987b17d)

375718 Google Chrome Prior To 91.0.4472.164 Multiple Vulnerabilities

375737 Microsoft Edge Based On Chromium Prior to 91.0.864.71 Multiple Vulnerabilities

500355 Alpine Linux Security Update for libxslt

501819 Alpine Linux Security Update for chromium

501913 Alpine Linux Security Update for qt5-qtwebengine

502173 Alpine Linux Security Update for qt5-qtwebengine

504119 Alpine Linux Security Update for libxslt

504614 Alpine Linux Security Update for chromium

672115 EulerOS Security Update for libxslt (EulerOS-SA-2022-2328)

672132 EulerOS Security Update for libxslt (EulerOS-SA-2022-2299)

672159 EulerOS Security Update for libxslt (EulerOS-SA-2022-2444)

672160 EulerOS Security Update for libxslt (EulerOS-SA-2022-2431)

672169 EulerOS Security Update for libxslt (EulerOS-SA-2022-2418)

672192 EulerOS Security Update for libxslt (EulerOS-SA-2022-2472)

672221 EulerOS Security Update for libxslt (EulerOS-SA-2022-2623)

710046 Gentoo Linux Chromium, Google Chrome Multiple Vulnerabilities (GLSA 202107-49)

710783 Gentoo Linux libxslt Multiple Vulnerabilities (GLSA 202310-23)

750873 OpenSUSE Security Update for chromium (openSUSE-SU-2021:1073-1)

750926 OpenSUSE Security Update for opera (openSUSE-SU-2021:1096-1)

750932 OpenSUSE Security Update for opera (openSUSE-SU-2021:1095-1)

751978 OpenSUSE Security Update for opera (openSUSE-SU-2022:0110-1)

753760 SUSE Enterprise Linux Security Update for libxslt (SUSE-SU-2023:0680-1)

753792 SUSE Enterprise Linux Security Update for libxslt (SUSE-SU-2023:0556-1)

901582 Common Base Linux Mariner (CBL-Mariner) Security Update for libxslt (9738)

901855 Common Base Linux Mariner (CBL-Mariner) Security Update for libxslt (9735)

902069 Common Base Linux Mariner (CBL-Mariner) Security Update for libxslt (9735-1)

902231 Common Base Linux Mariner (CBL-Mariner) Security Update for libxslt (9738-1)