CVE-2020-15810

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-15810
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-02 17:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Smugg

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Squid-cache	Squid	All	All	All	All
Application	Squid-cache	Squid	All	All	All	All

References

Reference	Source	Link	Tags
NetApp Product Security	CONFIRM	security.netapp.com	Broken
SQUID-2020:10 HTTP(S) Request Smuggling · Advisory · squid-cache/squid · GitHub	MISC	github.com	Mitigati
[SECURITY] Fedora 31 Update: squid-4.13-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third Pa
Debian -- Security Information -- DSA-4751-1 squid	DEBIAN	www.debian.org	Third Pa
[SECURITY] Fedora 33 Update: squid-4.13-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: squid-4.13-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third Pa
[security-announce] openSUSE-SU-2020:1346-1: critical: Security update f	SUSE	lists.opensuse.org	Mailing
[SECURITY] [DLA 2394-1] squid3 security update	MLIST	lists.debian.org	Mailing
USN-4551-1: Squid vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Pa
USN-4477-1: Squid vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	Third Pa
[SECURITY] Fedora 31 Update: squid-4.13-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
September 2020 Squid Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Pa
[SECURITY] Fedora 32 Update: squid-4.13-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
August 2020 Squid Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Pa
[security-announce] openSUSE-SU-2020:1369-1: critical: Security update f	SUSE	lists.opensuse.org	Mailing
[SECURITY] Fedora 33 Update: squid-4.13-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

356259 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-006

376993 Alibaba Cloud Linux Security Update for squid (ALINUX2-SA-2020:0119)

377360 Alibaba Cloud Linux Security Update for squid:4 (ALINUX3-SA-2022:0124)

500659 Alpine Linux Security Update for squid

501495 Alpine Linux Security Update for squid

504429 Alpine Linux Security Update for squid

753154 SUSE Enterprise Linux Security Update for squid (SUSE-SU-2022:14908-1)

960348 Rocky Linux Security Update for squid:4 (RLSA-2020:3623)

CVE.report and Source URL Uptime Status status.cve.report