CVE-2020-11945

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-11945
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-23 15:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain a

Risk And Classification

Problem Types: CWE-190

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	19.10	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	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Squid-cache	Squid	All	All	All	All
Application	Squid-cache	Squid	All	All	All	All
Application	Squid-cache	Squid	All	All	All	All
Application	Squid-cache	Squid	All	All	All	All

References

Reference

[SECURITY] Fedora 32 Update: squid-4.11-1.fc32 - package-announce - Fedora Mailing-Lists

Fix auth digest refcount integer overflow by desbma-s1n · Pull Request #585 · squid-cache/squid · GitHub

[SECURITY] Fedora 30 Update: squid-4.11-1.fc30 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2278-1] squid3 security update

oss-security - [ADVISORY] SQUID-2020:4 Multiple issues in HTTP Digest authentication

Bug 1170313 – VUL-0: CVE-2020-11945: squid: integer overflow bug allows credential replay and remote code execution attacks against HTT

[SECURITY] Fedora 32 Update: squid-4.11-1.fc32 - package-announce - Fedora Mailing-Lists

Fix auth digest refcount integer overflow (#585) · squid-cache/squid@eeebf0f · GitHub

[security-announce] openSUSE-SU-2020:0623-1: important: Security update

[SECURITY] Fedora 30 Update: squid-4.11-1.fc30 - package-announce - Fedora Mailing-Lists

Squid: Multiple vulnerabilities (GLSA 202005-05) — Gentoo security

CVE-2020-11945 Squid Vulnerability in NetApp Products | NetApp Product Security

www.squid-cache.org/Versions/v4/changesets/squid-4-eeebf0f37a72a2de08348e85ae34b0...

Debian -- Security Information -- DSA-4682-1 squid

[SECURITY] Fedora 31 Update: squid-4.11-1.fc31 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 31 Update: squid-4.11-1.fc31 - package-announce - Fedora Mailing-Lists

master.squid-cache.org/Versions/v4/changesets/squid-4-eeebf0f37a72a2de08348e85ae34b0...

USN-4356-1: Squid vulnerabilities | Ubuntu security notices | Ubuntu

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

296074 Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)

356292 Amazon Linux Security Advisory for squid : ALASSQUID4-2023-008

377033 Alibaba Cloud Linux Security Update for squid (ALINUX2-SA-2020:0092)

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

940334 AlmaLinux Security Update for squid:4 (ALSA-2020:2041)

960236 Rocky Linux Security Update for squid:4 (RLSA-2020:2041)

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