CVE-2020-13777

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-13777
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-04 07:15:00 UTC
Updated	2023-11-07 03:16:00 UTC
Description	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2,

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	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	10.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Gnu	Gnutls	All	All	All	All
Application	Gnu	Gnutls	All	All	All	All

References

Reference	Source	Link
USN-4384-1: GnuTLS vulnerability | Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.14-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE-2020-13777 GnuTLS Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com

GnuTLS: Information disclosure (GLSA 202006-01) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 32 Update: gnutls-3.6.14-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[security-announce] openSUSE-SU-2020:0790-1: important: Security update	SUSE	lists.opensuse.org
Debian -- Security Information -- DSA-4697-1 gnutls28	DEBIAN	www.debian.org
[SECURITY] Fedora 31 Update: mingw-gnutls-3.6.14-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
GnuTLS	CONFIRM	gnutls.org
[SECURITY] Fedora 31 Update: gnutls-3.6.14-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 31 Update: gnutls-3.6.14-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.14-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 32 Update: gnutls-3.6.14-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 31 Update: mingw-gnutls-3.6.14-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 296071 Oracle Solaris 11.4 Support Repository Update (SRU) 27.82.1 Missing (CPUOCT2020)
- 500233 Alpine Linux Security Update for gnutls
- 500361 Alpine Linux Security Update for gnutls
- 503979 Alpine Linux Security Update for gnutls
- 591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- 900228 CBL-Mariner Linux Security Update for gnutls 3.6.8
- 903575 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (1879)