CVE-2020-11501

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-11501
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-03 13:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected version is 3.6.3 (2018-07-16) beca

Risk And Classification

Problem Types: CWE-330

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	19.10	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	31	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
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 31 Update: mingw-gnutls-3.6.13-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedor
[SECURITY] Fedora 31 Update: mingw-gnutls-3.6.13-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor

GnuTLS	MISC	www.gnu
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedor
Debian -- Security Information -- DSA-4652-1 gnutls28	DEBIAN	www.deb
CVE-2020-11501 GnuTLS Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.n
[security-announce] openSUSE-SU-2020:0501-1: moderate: Security update f	SUSE	lists.open
CVE-2020-11501: DTLS client hello contains a random value of all zeroes (#960) · Issues · gnutls / GnuTLS · GitLab	MISC	gitlab.con
NEWS: updated for release (5b595e8e) · Commits · gnutls / GnuTLS · GitLab	MISC	gitlab.con
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedor
USN-4322-1: GnuTLS vulnerability | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubun
GnuTLS: DTLS protocol regression (GLSA 202004-06) — Gentoo security	GENTOO	security.g
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

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)
- 377363 Alibaba Cloud Linux Security Update for gnutls (ALINUX3-SA-2021:0008)
- 500232 Alpine Linux Security Update for gnutls
- 500360 Alpine Linux Security Update for gnutls
- 503978 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
- 903248 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (2186)