



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.org
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Debian -- Security Information -- DSA-4652-1 gnutls28	DEBIAN	www.debian.org
CVE-2020-11501 GnuTLS Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
[security-announce] openSUSE-SU-2020:0501-1: moderate: Security update for gnutls	SUSE	lists.opensuse.org
CVE-2020-11501: DTLS client hello contains a random value of all zeroes (#960) · Issues · gnutls / GnuTLS · GitLab	MISC	gitlab.com
NEWS: updated for release (5b595e8e) · Commits · gnutls / GnuTLS · GitLab	MISC	gitlab.com
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.13-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
USN-4322-1: GnuTLS vulnerability Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
GnuTLS: DTLS protocol regression (GLSA 202004-06) — Gentoo security	GENTOO	security.gentoo.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)
- [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)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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