



# CVE-2020-13777

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2020-13777  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2020-06-04 07:15:00 UTC   |
| <b>Updated</b>         | 2023-11-07 03:16:00 UTC   |
| <b>Description</b>     | 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 | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 19.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 20.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 19.10   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>     | <a href="#">Ubuntu Linux</a> | 20.04   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 31      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 32      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 32      | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Gnutls</a>       | All     | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Gnutls</a>       | All     | All    | All     | All      |

## References

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

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

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)

© [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](https://status.cve.report)