



# CVE-2020-24659

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

## Summary

<b>CVE</b>	CVE-2020-24659
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-04 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:20:00 UTC
<b>Description</b>	An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a

## Risk And Classification

**Problem Types:** CWE-787 | CWE-476

## 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>	20.04	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>	33	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
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 33 Update: mingw-gnutls-3.6.15-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
GnuTLS	MISC	<a href="https://www.gnutls.org">www.gnutls.org</a>
[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.15-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
GnuTLS: Denial of service (GLSA 202009-01) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
USN-4491-1: GnuTLS vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
CVE-2020-24659 GnuTLS Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>

[SECURITY] Fedora 32 Update: mingw-gnutls-3.6.15-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2020:1743-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 33 Update: mingw-gnutls-3.6.15-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2020:1724-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
CVE-2020-24659: read-heap-buffer-overflow found by fuzz (#1071) · Issues · gnutls / GnuTLS · GitLab	MISC	<a href="https://gitlab.com">gitlab.com</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

- [296070](#) Oracle Solaris 11.4 Support Repository Update (SRU) 28.82.3 Missing (CPUOCT2020)
- [377363](#) Alibaba Cloud Linux Security Update for gnutls (ALINUX3-SA-2021:0008)
- [500234](#) Alpine Linux Security Update for gnutls
- [500362](#) Alpine Linux Security Update for gnutls
- [503980](#) Alpine Linux Security Update for gnutls
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- [690514](#) Free Berkeley Software Distribution (FreeBSD) Security Update for gnutls (2272e6f1-f029-11ea-838a-0011d823eebd)
- [770068](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)
- [900113](#) CBL-Mariner Linux Security Update for gnutls 3.6.14
- [901708](#) Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (6445-1)
- [902834](#) Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (2201)
- [940380](#) AlmaLinux Security Update for gnutls (ALSA-2020:5483)

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)