CVE-2015-3308

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-3308
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-02 14:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Double free vulnerability in lib/x509/x509_ext.c in GnuTLS before 3.3.14 allows remote attackers to cause a denial of servic

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All

Application	Gnu	Gnutls	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
GnuTLS 'x509_ext.c' Use After Free Denial of Service Vulnerability
oss-security - double-free in gnutls (CRL distribution points parsing)
GnuTLS: Multiple vulnerabilities (GLSA 201506-03) — Gentoo security
[SECURITY] Fedora 22 Update: gnutls-3.3.14-1.fc22
eliminated double-free in the parsing of dist points (d6972be3) · Commits · gnutls / Gnutls · GitLab
GnuTLS Double-Free Memory Error in CRL Distribution Point Parsing Lets Remote Users Cause the Target Service to Crash - SecurityTracke
Better fix for the double free in dist point parsing (053ae654) · Commits · gnutls / Gnutls · GitLab
GnuTLS
oss-security - Re: double-free in gnutls (CRL distribution points parsing)
USN-2727-1: GnuTLS vulnerabilities | Ubuntu
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.