



CVE-2008-4989

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

Summary

CVE	CVE-2008-4989
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-11-13 01:00:01 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The _gnutls_x509_verify_certificate function in lib/x509/verify.c in libgnutls in GnuTLS before 2.6.1 trusts certificate chains i

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Problem Types: CWE-295 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Fedoraproject	Fedora	8	All	All	All
Operating System	Fedoraproject	Fedora	9	All	All	All
Application	Gnu	Gnutls	All	All	All	All
Operating System	Opensuse	Opensuse	All	All	All	All
Operating System	Suse	Linux Enterprise	10.0	-	All	All
Operating System	Suse	Linux Enterprise	11.0	-	All	All
Operating System	Suse	Linux Enterprise Server	10	-	All	All
Operating System	Suse	Linux Enterprise Server	11	-	All	All

Vendor Declared Affected Products

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

References	
Reference	Source
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661
Gentoo update for gnutls - Secunia.com	af854a3a-2127-422b-91ae-364da2661
Advisories:rPSA-2008-0322 - rPath Wiki	af854a3a-2127-422b-91ae-364da2661
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661
GnuTLS - GNU Project - Free Software Foundation	af854a3a-2127-422b-91ae-364da2661
GnuTLS X.509 Certificate Chain Validation Bug Permits Man-in-the-Middle Attacks - SecurityTracker	af854a3a-2127-422b-91ae-364da2661
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:027	af854a3a-2127-422b-91ae-364da2661
SecurityFocus	af854a3a-2127-422b-91ae-364da2661
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661
Debian update for gnutls13 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da2661
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661
Fedora update for gnutls - Secunia.com	af854a3a-2127-422b-91ae-364da2661
Gmane -- Mail To News And Back Again	af854a3a-2127-422b-91ae-364da2661
Ubuntu update for GnuTLS - Secunia.com	af854a3a-2127-422b-91ae-364da2661
GnuTLS: Certificate validation error — Gentoo Linux Documentation	af854a3a-2127-422b-91ae-364da2661
GnuTLS X.509 Certificate Chain Validation Vulnerability - Secunia.com	af854a3a-2127-422b-91ae-364da2661
GnuTLS X.509 Certificate Chain Security Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661
issues.rpath.com/browse/RPL-2886	af854a3a-2127-422b-91ae-364da2661
Red Hat update for gnutls - Secunia.com	af854a3a-2127-422b-91ae-364da2661
Sun Solaris GnuTLS X.509 Certificate Chain Validation Vulnerability - Secunia.com	af854a3a-2127-422b-91ae-364da2661
Support / Security / Advisories // MDVSA-2008:227 Mandriva	af854a3a-2127-422b-91ae-364da2661
Support	af854a3a-2127-422b-91ae-364da2661
USN-678-1: GnuTLS vulnerability Ubuntu security notices	af854a3a-2127-422b-91ae-364da2661
USN-678-2: GnuTLS regression Ubuntu	af854a3a-2127-422b-91ae-364da2661
sunsolve.sun.com/search/document.do	af854a3a-2127-422b-91ae-364da2661
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:009	af854a3a-2127-422b-91ae-364da2661
Debian -- Security Information -- DSA-1719-1 gnutls13	af854a3a-2127-422b-91ae-364da2661
[SECURITY] Fedora 9 Update: gnutls-2.0.4-4.fc9	af854a3a-2127-422b-91ae-364da2661
Gmane -- Mail To News And Back Again	af854a3a-2127-422b-91ae-364da2661
[SECURITY] Fedora 8 Update: gnutls-1.6.3-5.fc8	af854a3a-2127-422b-91ae-364da2661
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)