



CVE-2014-0092

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

Summary

CVE	CVE-2014-0092
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-07 00:10:53 UTC
Updated	2026-05-06 22:30:45 UTC
Description	lib/x509/verify.c in GnuTLS before 3.1.22 and 3.2.x before 3.2.12 does not properly handle unspecified errors when verifyin

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	3.1.0	All	All	All

Application	Gnu	Gnutls	3.1.1	All	All	All
Application	Gnu	Gnutls	3.1.10	All	All	All
Application	Gnu	Gnutls	3.1.11	All	All	All
Application	Gnu	Gnutls	3.1.12	All	All	All
Application	Gnu	Gnutls	3.1.13	All	All	All
Application	Gnu	Gnutls	3.1.14	All	All	All
Application	Gnu	Gnutls	3.1.15	All	All	All
Application	Gnu	Gnutls	3.1.16	All	All	All
Application	Gnu	Gnutls	3.1.17	All	All	All
Application	Gnu	Gnutls	3.1.18	All	All	All
Application	Gnu	Gnutls	3.1.19	All	All	All
Application	Gnu	Gnutls	3.1.2	All	All	All
Application	Gnu	Gnutls	3.1.20	All	All	All
Application	Gnu	Gnutls	3.1.3	All	All	All
Application	Gnu	Gnutls	3.1.4	All	All	All
Application	Gnu	Gnutls	3.1.5	All	All	All
Application	Gnu	Gnutls	3.1.6	All	All	All
Application	Gnu	Gnutls	3.1.7	All	All	All
Application	Gnu	Gnutls	3.1.8	All	All	All
Application	Gnu	Gnutls	3.1.9	All	All	All
Application	Gnu	Gnutls	3.2.0	All	All	All
Application	Gnu	Gnutls	3.2.1	All	All	All
Application	Gnu	Gnutls	3.2.10	All	All	All
Application	Gnu	Gnutls	3.2.2	All	All	All
Application	Gnu	Gnutls	3.2.3	All	All	All
Application	Gnu	Gnutls	3.2.4	All	All	All
Application	Gnu	Gnutls	3.2.5	All	All	All
Application	Gnu	Gnutls	3.2.6	All	All	All
Application	Gnu	Gnutls	3.2.7	All	All	All
Application	Gnu	Gnutls	3.2.8	All	All	All
Application	Gnu	Gnutls	3.2.8.1	All	All	All
Application	Gnu	Gnutls	3.2.9	All	All	All
Application	Gnu	Gnutls	All	All	All	All
Application	Gnu	Gnutls	All	All	All	All

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

References

Reference	Source
USN-2127-1: GnuTLS vulnerability Ubuntu	af854a3a-2127-422b-91ae-3
[security-announce] openSUSE-SU-2014:0328-1: critical: gnutls: fixed SSL	af854a3a-2127-422b-91ae-3
[security-announce] SUSE-SU-2014:0324-1: critical: Security update for g	af854a3a-2127-422b-91ae-3
[security-announce] SUSE-SU-2014:0322-1: critical: Security update for g	af854a3a-2127-422b-91ae-3
Security Advisory SA56933 - Ubuntu update for gnutls26 - Secunia	af854a3a-2127-422b-91ae-3
Security Advisory SA57321 - Red Hat update for gnutls - Secunia	af854a3a-2127-422b-91ae-3
Red Hat Customer Portal	af854a3a-2127-422b-91ae-3
[security-announce] SUSE-SU-2014:0320-1: critical: Security update for g	af854a3a-2127-422b-91ae-3
Security Advisory SA57260 - SUSE update for gnutls - Secunia	af854a3a-2127-422b-91ae-3
Security Advisory SA57204 - Debian update for gnutls26 - Secunia	af854a3a-2127-422b-91ae-3
About Secunia Research Flexera	af854a3a-2127-422b-91ae-3
Debian -- Security Information -- DSA-2869-1 gnutls26	af854a3a-2127-422b-91ae-3
GnuTLS	af854a3a-2127-422b-91ae-3
Red Hat Customer Portal	af854a3a-2127-422b-91ae-3
Red Hat Customer Portal	af854a3a-2127-422b-91ae-3
[security-announce] SUSE-SU-2014:0319-1: critical: Security update for g	af854a3a-2127-422b-91ae-3
Security Advisory SA57274 - SUSE update for gnutls - Secunia	af854a3a-2127-422b-91ae-3
[security-announce] SUSE-SU-2014:0321-1: critical: Security update for g	af854a3a-2127-422b-91ae-3
Security Advisory SA57254 - SUSE update for gnutls - Secunia	af854a3a-2127-422b-91ae-3
[security-announce] openSUSE-SU-2014:0346-1: critical: gnutls	af854a3a-2127-422b-91ae-3
[security-announce] SUSE-SU-2014:0323-1: critical: Security update for g	af854a3a-2127-422b-91ae-3
GnuTLS CVE-2014-0092 Certificate Validation Security Bypass Vulnerability	af854a3a-2127-422b-91ae-3
[security-announce] SUSE-SU-2014:0445-1: important: Security update for	af854a3a-2127-422b-91ae-3
[security-announce] openSUSE-SU-2014:0325-1: critical: gnutls: fixed SSL	af854a3a-2127-422b-91ae-3
Red Hat Customer Portal	af854a3a-2127-422b-91ae-3
Bug 1069865 – CVE-2014-0092 gnutls: incorrect error handling in certificate verification (GNUTLS-SA-2014-2)	af854a3a-2127-422b-91ae-3
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](#)