



CVE-2012-1573

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

Summary

CVE	CVE-2012-1573
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-26 19:55:00 UTC
Updated	2023-11-07 02:10:00 UTC
Description	gnutls_cipher.c in libgnutls in GnuTLS before 2.12.17 and 3.x before 3.0.15 does not properly handle data encrypted with a

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	2.0.0	All	All	All
Application	Gnu	Gnutls	2.0.1	All	All	All
Application	Gnu	Gnutls	2.0.2	All	All	All
Application	Gnu	Gnutls	2.0.3	All	All	All
Application	Gnu	Gnutls	2.0.4	All	All	All
Application	Gnu	Gnutls	2.1.0	All	All	All
Application	Gnu	Gnutls	2.1.1	All	All	All
Application	Gnu	Gnutls	2.1.2	All	All	All
Application	Gnu	Gnutls	2.1.3	All	All	All
Application	Gnu	Gnutls	2.1.4	All	All	All
Application	Gnu	Gnutls	2.1.5	All	All	All
Application	Gnu	Gnutls	2.1.6	All	All	All
Application	Gnu	Gnutls	2.1.7	All	All	All
Application	Gnu	Gnutls	2.1.8	All	All	All
Application	Gnu	Gnutls	2.10.0	All	All	All
Application	Gnu	Gnutls	2.10.1	All	All	All
Application	Gnu	Gnutls	2.10.2	All	All	All

Application	Gnu	Gnutls	2.10.3	All	All	All
Application	Gnu	Gnutls	2.10.4	All	All	All
Application	Gnu	Gnutls	2.10.5	All	All	All
Application	Gnu	Gnutls	2.12.0	All	All	All
Application	Gnu	Gnutls	2.12.1	All	All	All
Application	Gnu	Gnutls	2.12.10	All	All	All
Application	Gnu	Gnutls	2.12.11	All	All	All
Application	Gnu	Gnutls	2.12.12	All	All	All
Application	Gnu	Gnutls	2.12.13	All	All	All
Application	Gnu	Gnutls	2.12.14	All	All	All
Application	Gnu	Gnutls	2.12.15	All	All	All
Application	Gnu	Gnutls	2.12.2	All	All	All
Application	Gnu	Gnutls	2.12.3	All	All	All
Application	Gnu	Gnutls	2.12.4	All	All	All
Application	Gnu	Gnutls	2.12.5	All	All	All
Application	Gnu	Gnutls	2.12.6	All	All	All
Application	Gnu	Gnutls	2.12.6.1	All	All	All
Application	Gnu	Gnutls	2.12.7	All	All	All
Application	Gnu	Gnutls	2.12.8	All	All	All
Application	Gnu	Gnutls	2.12.9	All	All	All
Application	Gnu	Gnutls	2.2.0	All	All	All
Application	Gnu	Gnutls	2.2.1	All	All	All
Application	Gnu	Gnutls	2.2.2	All	All	All
Application	Gnu	Gnutls	2.2.3	All	All	All
Application	Gnu	Gnutls	2.2.4	All	All	All
Application	Gnu	Gnutls	2.2.5	All	All	All
Application	Gnu	Gnutls	2.3.0	All	All	All
Application	Gnu	Gnutls	2.3.1	All	All	All
Application	Gnu	Gnutls	2.3.10	All	All	All
Application	Gnu	Gnutls	2.3.11	All	All	All
Application	Gnu	Gnutls	2.3.2	All	All	All
Application	Gnu	Gnutls	2.3.3	All	All	All
Application	Gnu	Gnutls	2.3.4	All	All	All
Application	Gnu	Gnutls	2.3.5	All	All	All
Application	Gnu	Gnutls	2.3.6	All	All	All

Application	Gnu	Gnutls	2.3.7	All	All	All
Application	Gnu	Gnutls	2.3.8	All	All	All
Application	Gnu	Gnutls	2.3.9	All	All	All
Application	Gnu	Gnutls	2.4.0	All	All	All
Application	Gnu	Gnutls	2.4.1	All	All	All
Application	Gnu	Gnutls	2.4.2	All	All	All
Application	Gnu	Gnutls	2.4.3	All	All	All
Application	Gnu	Gnutls	2.5.0	All	All	All
Application	Gnu	Gnutls	2.6.0	All	All	All
Application	Gnu	Gnutls	2.6.1	All	All	All
Application	Gnu	Gnutls	2.6.2	All	All	All
Application	Gnu	Gnutls	2.6.3	All	All	All
Application	Gnu	Gnutls	2.6.4	All	All	All
Application	Gnu	Gnutls	2.6.5	All	All	All
Application	Gnu	Gnutls	2.6.6	All	All	All
Application	Gnu	Gnutls	2.7.4	All	All	All
Application	Gnu	Gnutls	2.8.0	All	All	All
Application	Gnu	Gnutls	2.8.1	All	All	All
Application	Gnu	Gnutls	2.8.2	All	All	All
Application	Gnu	Gnutls	2.8.3	All	All	All
Application	Gnu	Gnutls	2.8.4	All	All	All
Application	Gnu	Gnutls	2.8.5	All	All	All
Application	Gnu	Gnutls	2.8.6	All	All	All
Application	Gnu	Gnutls	3.0	All	All	All
Application	Gnu	Gnutls	3.0.0	All	All	All
Application	Gnu	Gnutls	3.0.1	All	All	All
Application	Gnu	Gnutls	3.0.10	All	All	All
Application	Gnu	Gnutls	3.0.11	All	All	All
Application	Gnu	Gnutls	3.0.12	All	All	All
Application	Gnu	Gnutls	3.0.13	All	All	All
Application	Gnu	Gnutls	3.0.14	All	All	All
Application	Gnu	Gnutls	3.0.2	All	All	All
Application	Gnu	Gnutls	3.0.3	All	All	All
Application	Gnu	Gnutls	3.0.4	All	All	All
Application	Gnu	Gnutls	3.0.5	All	All	All
Application	Gnu	Gnutls	3.0.6	All	All	All

Application	Gnu	Gnutls	3.0.6	All	All	All
Application	Gnu	Gnutls	3.0.7	All	All	All
Application	Gnu	Gnutls	3.0.8	All	All	All
Application	Gnu	Gnutls	3.0.9	All	All	All
Application	Gnu	Gnutls	2.0.0	All	All	All
Application	Gnu	Gnutls	2.0.1	All	All	All
Application	Gnu	Gnutls	2.0.2	All	All	All
Application	Gnu	Gnutls	2.0.3	All	All	All
Application	Gnu	Gnutls	2.0.4	All	All	All
Application	Gnu	Gnutls	2.1.0	All	All	All
Application	Gnu	Gnutls	2.1.1	All	All	All
Application	Gnu	Gnutls	2.1.2	All	All	All
Application	Gnu	Gnutls	2.1.3	All	All	All
Application	Gnu	Gnutls	2.1.4	All	All	All
Application	Gnu	Gnutls	2.1.5	All	All	All
Application	Gnu	Gnutls	2.1.6	All	All	All
Application	Gnu	Gnutls	2.1.7	All	All	All
Application	Gnu	Gnutls	2.1.8	All	All	All
Application	Gnu	Gnutls	2.10.0	All	All	All
Application	Gnu	Gnutls	2.10.1	All	All	All
Application	Gnu	Gnutls	2.10.2	All	All	All
Application	Gnu	Gnutls	2.10.3	All	All	All
Application	Gnu	Gnutls	2.10.4	All	All	All
Application	Gnu	Gnutls	2.10.5	All	All	All
Application	Gnu	Gnutls	2.12.0	All	All	All
Application	Gnu	Gnutls	2.12.1	All	All	All
Application	Gnu	Gnutls	2.12.10	All	All	All
Application	Gnu	Gnutls	2.12.11	All	All	All
Application	Gnu	Gnutls	2.12.12	All	All	All
Application	Gnu	Gnutls	2.12.13	All	All	All
Application	Gnu	Gnutls	2.12.14	All	All	All
Application	Gnu	Gnutls	2.12.15	All	All	All
Application	Gnu	Gnutls	2.12.2	All	All	All
Application	Gnu	Gnutls	2.12.3	All	All	All
Application	Gnu	Gnutls	2.12.4	All	All	All
Application	Gnu	Gnutls	2.12.5	All	All	All

Application	Gnu	Gnutls	2.12.6	All	All	All
Application	Gnu	Gnutls	2.12.6.1	All	All	All
Application	Gnu	Gnutls	2.12.7	All	All	All
Application	Gnu	Gnutls	2.12.8	All	All	All
Application	Gnu	Gnutls	2.12.9	All	All	All
Application	Gnu	Gnutls	2.2.0	All	All	All
Application	Gnu	Gnutls	2.2.1	All	All	All
Application	Gnu	Gnutls	2.2.2	All	All	All
Application	Gnu	Gnutls	2.2.3	All	All	All
Application	Gnu	Gnutls	2.2.4	All	All	All
Application	Gnu	Gnutls	2.2.5	All	All	All
Application	Gnu	Gnutls	2.3.0	All	All	All
Application	Gnu	Gnutls	2.3.1	All	All	All
Application	Gnu	Gnutls	2.3.10	All	All	All
Application	Gnu	Gnutls	2.3.11	All	All	All
Application	Gnu	Gnutls	2.3.2	All	All	All
Application	Gnu	Gnutls	2.3.3	All	All	All
Application	Gnu	Gnutls	2.3.4	All	All	All
Application	Gnu	Gnutls	2.3.5	All	All	All
Application	Gnu	Gnutls	2.3.6	All	All	All
Application	Gnu	Gnutls	2.3.7	All	All	All
Application	Gnu	Gnutls	2.3.8	All	All	All
Application	Gnu	Gnutls	2.3.9	All	All	All
Application	Gnu	Gnutls	2.4.0	All	All	All
Application	Gnu	Gnutls	2.4.1	All	All	All
Application	Gnu	Gnutls	2.4.2	All	All	All
Application	Gnu	Gnutls	2.4.3	All	All	All
Application	Gnu	Gnutls	2.5.0	All	All	All
Application	Gnu	Gnutls	2.6.0	All	All	All
Application	Gnu	Gnutls	2.6.1	All	All	All
Application	Gnu	Gnutls	2.6.2	All	All	All
Application	Gnu	Gnutls	2.6.3	All	All	All
Application	Gnu	Gnutls	2.6.4	All	All	All
Application	Gnu	Gnutls	2.6.5	All	All	All
Application	Gnu	Gnutls	2.6.6	All	All	All

Application	Gnu	Gnutls	2.7.4	All	All	All
Application	Gnu	Gnutls	2.8.0	All	All	All
Application	Gnu	Gnutls	2.8.1	All	All	All
Application	Gnu	Gnutls	2.8.2	All	All	All
Application	Gnu	Gnutls	2.8.3	All	All	All
Application	Gnu	Gnutls	2.8.4	All	All	All
Application	Gnu	Gnutls	2.8.5	All	All	All
Application	Gnu	Gnutls	2.8.6	All	All	All
Application	Gnu	Gnutls	3.0	All	All	All
Application	Gnu	Gnutls	3.0.0	All	All	All
Application	Gnu	Gnutls	3.0.1	All	All	All
Application	Gnu	Gnutls	3.0.10	All	All	All
Application	Gnu	Gnutls	3.0.11	All	All	All
Application	Gnu	Gnutls	3.0.12	All	All	All
Application	Gnu	Gnutls	3.0.13	All	All	All
Application	Gnu	Gnutls	3.0.14	All	All	All
Application	Gnu	Gnutls	3.0.2	All	All	All
Application	Gnu	Gnutls	3.0.3	All	All	All
Application	Gnu	Gnutls	3.0.4	All	All	All
Application	Gnu	Gnutls	3.0.5	All	All	All
Application	Gnu	Gnutls	3.0.6	All	All	All
Application	Gnu	Gnutls	3.0.7	All	All	All
Application	Gnu	Gnutls	3.0.8	All	All	All
Application	Gnu	Gnutls	3.0.9	All	All	All
Application	Gnu	Gnutls	All	All	All	All

References						
Reference					Source	Link
[security-announce] SUSE-SU-2014:0320-1: critical: Security update for g					SUSE	lists.opensuse.org
oss-security - CVE request: GnuTLS TLS record handling issue / MU-201202-01					MLIST	www.openwall.com
Red Hat Customer Portal					REDHAT	rhn.redhat.com
Savannah Git Hosting - gnutls.git/commit						git.savannah.gnu.org
Security Advisory SA48511 - Debian update for gnutls26 - Secunia					SECUNIA	secunia.com
USN-1418-1: GnuTLS vulnerabilities Ubuntu					UBUNTU	www.ubuntu.com
GnuTLS Error in ciphertext_to_compressed() Lets Remote Users Deny Service - SecurityTracker					SECTRACK	www.securitytracker.com
20120320 Mu Dynamics, Inc. Security Advisories MU-201202-01 and MU-201202-02 for GnuTLS and Libtasn1					BUGTRAQ	archives.neohaps.org

Bug 805432 – CVE-2012-1573 gnutls: TLS record handling issue (GNUTLS-SA-2012-2, MU-201202-01)	CONFIRM	bugzilla.redhat.com
Savannah Git Hosting - gnutls.git/commit	CONFIRM	git.savannah.gnu.org
Gmane -- gnutls 3.0.15	MLIST	article.gmane.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Gmane -- Mail To News And Back Again	MLIST	article.gmane.org
Savannah Git Hosting - gnutls.git/commit		git.savannah.gnu.org
GnuTLS - GNU Project - Free Software Foundation	CONFIRM	www.gnu.org
[SECURITY] Fedora 16 Update: gnutls-2.12.14-2.fc16	FEDORA	lists.fedoraproject.org
Red Hat Customer Portal	REDHAT	rhn.redhat.com
GnuTLS TLS Record Handling Heap Memory Corruption Vulnerability	BID	www.securityfocus.com
oss-security - Re: CVE request: GnuTLS TLS record handling issue / MU-201202-01	MLIST	www.openwall.com
Security Alerts - Secunia	SECUNIA	secunia.com
Security Advisory SA57260 - SUSE update for gnutls - Secunia	SECUNIA	secunia.com
Security Advisory SA48712 - Ubuntu update for gnutls26 - Secunia	SECUNIA	secunia.com
www.mandriva.com	MANDRIVA	www.mandriva.com
[SECURITY] Fedora 15 Update: gnutls-2.10.5-3.fc15	FEDORA	lists.fedoraproject.org
80259	OSVDB	osvdb.org
About Secunia Research Flexera	SECUNIA	secunia.com
Debian -- Security Information -- DSA-2441-1 gnutls26	DEBIAN	www.debian.org
Savannah Git Hosting - gnutls.git/commit	CONFIRM	git.savannah.gnu.org
Mu Dynamics Blog » Security Advisories MU-201202-01 and MU-201202-02 for GnuTLS and Libtasn1	MISC	blog.mudynamics.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)