



CVE-2014-3466

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

Summary

CVE	CVE-2014-3466
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-03 14:55:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.4.x before 3.4.10 allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via a long certificate.

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

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	3.1.21	All	All	All
Application	Gnu	Gnutls	3.1.22	All	All	All
Application	Gnu	Gnutls	3.1.23	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	3.2.11	All	All	All
Application	Gnu	Gnutls	3.2.12	All	All	All
Application	Gnu	Gnutls	3.2.12.1	All	All	All
Application	Gnu	Gnutls	3.2.13	All	All	All
Application	Gnu	Gnutls	3.2.14	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	3.3.0	-	All	All
Application	Gnu	Gnutls	3.3.0	pre0	All	All
Application	Gnu	Gnutls	3.3.1	All	All	All
Application	Gnu	Gnutls	3.3.2	All	All	All
Application	Gnu	Gnutls	3.3.3	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
linux.oracle.com ELSA-2014-0594 - gnutls security update
Security Advisory SA58642 - Red Hat update for gnutls - Secunia
Security Advisory SA59016 - Ubuntu update for gnutls26 - Secunia
Security Advisory SA59838 - IBM SmartCloud Provisioning for IBM Provided Software Virtual Appliance GnuTLS Vulnerability - Secunia
Security Advisory SA59408 - Novell Open Enterprise Server GnuTLS Multiple Vulnerabilities - Secunia
IBM Support
www.novell.com/support/kb/doc.php
GnuTLS Server Hello Session ID Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker
[security-announce] SUSE-SU-2014:0758-1: important: Security update for
Bug 1101932 – CVE-2014-3466 gnutls: insufficient session id length check in _gnutls_read_server_hello (GNUTLS-SA-2014-3)
Security Advisory SA58340 - GnuTLS "read_server_hello()" Memory Corruption Vulnerability - Secunia
Red Hat Customer Portal
Security Advisory SA58601 - Oracle Linux update for gnutls - Secunia
Technical Analysis Of The GnuTLS Hello Vulnerability
Red Hat Customer Portal
GnuTLS 'gnutls_handshake.c' Memory Corruption Vulnerability
IBM Security Bulletin: Vulnerability in Gnu Transport Layer Security (GnuTLS) affects IBM SmartCloud Provisioning 2.1 for IBM Provided Softw
Security Advisory SA58598 - Debian update for gnutls26 - Secunia
[security-announce] SUSE-SU-2014:0788-1: important: Security update for

Red Hat Customer Portal
Security Advisory SA60384 - IBM Flex System Manager Node (FSM) GnuTLS Memory Corruption Vulnerability - Secunia
[security-announce] openSUSE-SU-2014:0763-1: important: gnutls: Fixed po
Red Hat Customer Portal
www.novell.com/support/kb/doc.php
Debian -- Security Information -- DSA-2944-1 gnutls26
About Secunia Research Flexera
Security Advisory SA59021 - Oracle Linux update for gnutls - Secunia
linux.oracle.com ELSA-2014-0595 - gnutls security update
Security Advisory SA59086 - SUSE update for gnutls - Secunia
USN-2229-1: GnuTLS vulnerability Ubuntu
GnuTLS
[security-announce] openSUSE-SU-2014:0767-1: important: gnutls: Fixed po
Prevent memory corruption due to server hello parsing. - Gitorious
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.