



CVE-2006-4790

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

Summary

CVE	CVE-2006-4790
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-14 19:07:00 UTC
Updated	2017-10-11 01:31:00 UTC
Description	verify.c in GnuTLS before 1.4.4, when using an RSA key with exponent 3, does not properly handle excess data in the dige

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

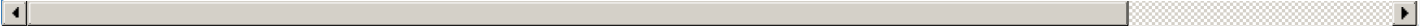
Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Gnutls	1.0.17	All	All	All
Application	Gnu	Gnutls	1.0.18	All	All	All
Application	Gnu	Gnutls	1.0.19	All	All	All
Application	Gnu	Gnutls	1.0.20	All	All	All
Application	Gnu	Gnutls	1.0.21	All	All	All
Application	Gnu	Gnutls	1.0.22	All	All	All
Application	Gnu	Gnutls	1.0.23	All	All	All
Application	Gnu	Gnutls	1.0.24	All	All	All
Application	Gnu	Gnutls	1.0.25	All	All	All
Application	Gnu	Gnutls	1.1.14	All	All	All
Application	Gnu	Gnutls	1.1.15	All	All	All
Application	Gnu	Gnutls	1.1.16	All	All	All
Application	Gnu	Gnutls	1.1.17	All	All	All
Application	Gnu	Gnutls	1.1.18	All	All	All
Application	Gnu	Gnutls	1.1.19	All	All	All
Application	Gnu	Gnutls	1.1.20	All	All	All
Application	Gnu	Gnutls	1.1.21	All	All	All

Application	Gnu	Gnutls	1.1.22	All	All	All
Application	Gnu	Gnutls	1.1.23	All	All	All
Application	Gnu	Gnutls	1.2.0	All	All	All
Application	Gnu	Gnutls	1.2.1	All	All	All
Application	Gnu	Gnutls	1.2.10	All	All	All
Application	Gnu	Gnutls	1.2.11	All	All	All
Application	Gnu	Gnutls	1.2.2	All	All	All
Application	Gnu	Gnutls	1.2.3	All	All	All
Application	Gnu	Gnutls	1.2.4	All	All	All
Application	Gnu	Gnutls	1.2.5	All	All	All
Application	Gnu	Gnutls	1.2.6	All	All	All
Application	Gnu	Gnutls	1.2.7	All	All	All
Application	Gnu	Gnutls	1.2.8	All	All	All
Application	Gnu	Gnutls	1.2.8.1a1	All	All	All
Application	Gnu	Gnutls	1.2.9	All	All	All
Application	Gnu	Gnutls	1.3.0	All	All	All
Application	Gnu	Gnutls	1.3.1	All	All	All
Application	Gnu	Gnutls	1.3.2	All	All	All
Application	Gnu	Gnutls	1.3.3	All	All	All
Application	Gnu	Gnutls	1.3.4	All	All	All
Application	Gnu	Gnutls	1.3.5	All	All	All
Application	Gnu	Gnutls	1.4.0	All	All	All
Application	Gnu	Gnutls	1.4.1	All	All	All
Application	Gnu	Gnutls	1.0.17	All	All	All
Application	Gnu	Gnutls	1.0.18	All	All	All
Application	Gnu	Gnutls	1.0.19	All	All	All
Application	Gnu	Gnutls	1.0.20	All	All	All
Application	Gnu	Gnutls	1.0.21	All	All	All
Application	Gnu	Gnutls	1.0.22	All	All	All
Application	Gnu	Gnutls	1.0.23	All	All	All
Application	Gnu	Gnutls	1.0.24	All	All	All
Application	Gnu	Gnutls	1.0.25	All	All	All
Application	Gnu	Gnutls	1.1.14	All	All	All
Application	Gnu	Gnutls	1.1.15	All	All	All
Application	Gnu	Gnutls	1.1.16	All	All	All

Application	Gnu	Gnutls	1.1.17	All	All	All
Application	Gnu	Gnutls	1.1.18	All	All	All
Application	Gnu	Gnutls	1.1.19	All	All	All
Application	Gnu	Gnutls	1.1.20	All	All	All
Application	Gnu	Gnutls	1.1.21	All	All	All
Application	Gnu	Gnutls	1.1.22	All	All	All
Application	Gnu	Gnutls	1.1.23	All	All	All
Application	Gnu	Gnutls	1.2.0	All	All	All
Application	Gnu	Gnutls	1.2.1	All	All	All
Application	Gnu	Gnutls	1.2.10	All	All	All
Application	Gnu	Gnutls	1.2.11	All	All	All
Application	Gnu	Gnutls	1.2.2	All	All	All
Application	Gnu	Gnutls	1.2.3	All	All	All
Application	Gnu	Gnutls	1.2.4	All	All	All
Application	Gnu	Gnutls	1.2.5	All	All	All
Application	Gnu	Gnutls	1.2.6	All	All	All
Application	Gnu	Gnutls	1.2.7	All	All	All
Application	Gnu	Gnutls	1.2.8	All	All	All
Application	Gnu	Gnutls	1.2.8.1a1	All	All	All
Application	Gnu	Gnutls	1.2.9	All	All	All
Application	Gnu	Gnutls	1.3.0	All	All	All
Application	Gnu	Gnutls	1.3.1	All	All	All
Application	Gnu	Gnutls	1.3.2	All	All	All
Application	Gnu	Gnutls	1.3.3	All	All	All
Application	Gnu	Gnutls	1.3.4	All	All	All
Application	Gnu	Gnutls	1.3.5	All	All	All
Application	Gnu	Gnutls	1.4.0	All	All	All
Application	Gnu	Gnutls	1.4.1	All	All	All

References						
Reference				Source	Link	
Advisories - Mandriva Linux				MANDRIVA	www.mandriva.com	
SUSE Update for Multiple Packages - Advisories - Secunia				SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.com	
GnuTLS RSA Signature Forgery Vulnerability - Advisories - Secunia				SECUNIA	secunia.com	
Mandriva update for gnutls - Secunia.com				SECUNIA	secunia.com	

Security Announcement	SUSE	www.novell.com
Debian update for gnutls11 / gnutls13 - Secunia.com	SECUNIA	secunia.com
Webmail - OVH	VUPEN	www.vupen.com
[gnutls-dev] Variant of Bleichenbacher's crypto 06 rump session attack	MLIST	lists.gnupg.org
SecurityTracker.com Archives - GnuTLS May Allow Digital Signatures to Be Forged	SECTrack	securitytracker.com
Red Hat update for gnutls - Advisories - Secunia	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.co
Gentoo update for gnutls - Advisories - Secunia	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Avaya CMS Sun Solaris X Display Manager Security Issue - Advisories - Secunia	SECUNIA	secunia.com
GnuTLS - GNU Project - Free Software Foundation	CONFIRM	www.gnu.org
usn/usn-348-1 - Ubuntu: Linux for human beings	UBUNTU	www.ubuntu.com
Support	REDHAT	www.redhat.com
GnuTLS: RSA Signature Forgery — Gentoo Linux Documentation	GENTOO	security.gentoo.org
Sun Solaris GnuTLS RSA Signature Forgery Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-1182-1 gnutls11	DEBIAN	www.debian.org
102970	SUNALERT	sunsolve.sun.com
[gnutls-dev] Re: Variant of Bleichenbacher's crypto 06 rump session attack	MLIST	lists.gnupg.org
#102648: Security Vulnerability in RSA Signature Verification Impacting Multiple SUN Products	SUNALERT	sunsolve.sun.com
Security Announcement	SUSE	www.novell.com
Ubuntu update for gnutls - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
ASA-2006-250 (SUN 102606, 102636, 102640, 102648, 102651, 102652, 102655, 102657)	CONFIRM	support.avaya.com
GNUTLS PKCS RSA Signature Forgery Vulnerability	BID	www.securityfocus.com
Sun Solaris RSA Signature Forgery Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Webmail - OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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

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