CVE-2005-2700

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2005-2700
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-09-06 23:03:00 UTC
Updated	2023-02-13 01:16:00 UTC
Description	ssl_engine_kernel.c in mod_ssl before 2.8.24, when using "SSLVerifyClient optional" in the global virtual host configuration.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	Apache	Http Server	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All

Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.54	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.1	All	All	All
Application	Apache	Http Server	2.1.1	All	All	All
Application	Apache	Http Server	2.1.2	All	All	All
Application	Apache	Http Server	2.1.3	All	All	All
Application	Apache	Http Server	2.1.4	All	All	All
Application	Apache	Http Server	2.1.5	All	All	All
Application	Apache	Http Server	2.1.6	All	All	All
Application	Apache	Http Server	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All

Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.54	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.1	All	All	All
Application	Apache	Http Server	2.1.1	All	All	All
Application	Apache	Http Server	2.1.2	All	All	All
Application	Apache	Http Server	2.1.3	All	All	All
Application	Apache	Http Server	2.1.4	All	All	All
Application	Apache	Http Server	2.1.5	All	All	All
Application	Apache	Http Server	2.1.6	All	All	All
Operating System	Canonical	Ubuntu Linux	4.10	All	All	All
Operating System	Canonical	Ubuntu Linux	5.04	All	All	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.0.15	All	All	All
Application	Mod Ssl	Mod Ssl	2.1.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.2.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.3.11	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.10	All	All	All
Application	Mod Ssl	Mod Ssl	2.5.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.7.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.14	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.15	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.16	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.18	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.19	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.20	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.21	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.22	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.23	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.24	All	All	All

Application	Mod Ssl	Mod Ssl	2.0.15	All	All	All
Application	Mod Ssl	Mod Ssl	2.1.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.2.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.3.11	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.10	All	All	All
Application	Mod Ssl	Mod Ssl	2.5.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.7.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.14	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.15	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.16	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.18	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.19	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.20	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.21	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.22	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.23	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.24	All	All	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All

References

Reference	Source	Link
Pony Mail!	MLIST	lists.apache.org
Secunia - Advisories - Mac OS X Security Update Fixes Multiple Vulnerabilities	SECUNIA	secunia.com
Secunia - Advisories - Sun Solaris Multiple Apache2 Vulnerabilities	SECUNIA	secunia.com
Secunia - Advisories - Mandriva update for apache2	SECUNIA	secunia.com
Pony Mail!	MISC	lists.apache.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MISC	lists.apache.org
1. Overview:	CONFIRM	support.avaya.com
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
usn/usn-177-1 - Ubuntu Linux	UBUNTU	www.ubuntu.com
Secunia - Advisories - Gentoo update for apache/mod_ssl	SECUNIA	secunia.com
'[OpenPKG-SA-2005.017] OpenPKG Security Advisory (modssl)' - MARC	OPENPKG	marc.info
Apache Mod_SSL SSLVerifyClient Restriction Bypass Vulnerability	BID	www.securityfocus.com
Secunia - Advisories - Sun Solaris Multiple Apache Vulnerabilities	SECUNIA	secunia.com
TSLSA-2005-0059 - multi	TRUSTIX	lists.trustix.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
people.apache.org/~jorton/CAN-2005-2700.diff	CONFIRM	people.apache.org
Pony Mail!	MISC	lists.apache.org
Secunia - Advisories - Ubuntu Updates for Multiple Packages	SECUNIA	secunia.com
Secunia - Advisories - Red Hat Stronghold Multiple Vulnerabilities	SECUNIA	secunia.com
Security Announcement	SUSE	www.novell.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Secunia - Advisories - Trustix update for multiple packages	SECUNIA	secunia.com
Bug 167195 – CAN-2005-2700 SSLVerifyClient flaw	CONFIRM	bugzilla.redhat.com
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com
IBM - Subscription service - Bulletin	CONFIRM	www14.software.ibm.com

IBM - Subscription service - Bulletin	CONFIRM	www14.software.ibm.com
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	SECUNIA	secunia.com
Webmail - OVH	VUPEN	www.vupen.com
Secunia - Advisories - Fedora update for httpd	SECUNIA	secunia.com
'[ANNOUNCE] mod_ssl 2.8.24-1.3.33' - MARC	MLIST	marc.info
Pony Mail!	MISC	lists.apache.org
Secunia - Advisories - Debian update for libapache-mod-ssl	SECUNIA	secunia.com
Repository / Oval Repository	OVAL	oval.cisecurity.org
Secunia - Advisories - Trustix update for multiple packages	SECUNIA	secunia.com
Secunia - Advisories - mod_ssl "SSLVerifyClient" Security Bypass Security Issue	SECUNIA	secunia.com
Secunia - Advisories - Red Hat update for httpd/mod_ssl	SECUNIA	secunia.com
Pony Mail!	MLIST	lists.apache.org
#102198: Security Vulnerabilities in the Apache 2 Web Server	SUNALERT	sunsolve.sun.com
Pony Mail!	MLIST	lists.apache.org
Gentoo Linux Documentation -- Apache, mod_ssl: Multiple vulnerabilities	GENTOO	www.gentoo.org
Advisories - Mandriva	MANDRIVA	www.mandriva.com
Pony Mail!	MISC	lists.apache.org
Security Announcement	SUSE	www.novell.com
SUSE Security Announcement: Apache2 security problems (SUSE-SA:2006:051)	SUSE	lists.opensuse.org
'[security bulletin] SSRT051043 rev.0 - Apache Remote Unauthorized access' - MARC	HP	marc.info
Secunia - Advisories - Slackware update for mod_ssl	SECUNIA	secunia.com
Pony Mail!	MLIST	lists.apache.org
Secunia - Advisories - Debian update for apache2	SECUNIA	secunia.com
IBM HMC Apache2 / OpenSSL Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com
Debian -- Security Information -- DSA-807-1 libapache-mod-ssl	DEBIAN	www.debian.org
Secunia - Advisories - HP-UX Apache mod_ssl "SSLVerifyClient" Security Bypass Security Issue	SECUNIA	secunia.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
19188	OSVDB	www.osvdb.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
SUSE update for apache2 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Pony Mail!	MLIST	lists.apache.org
Secunia - Advisories - SUSE update for apache2	SECUNIA	secunia.com
Debian -- Security Information -- DSA-805-1 apache2	DEBIAN	www.debian.org
Pony Mail!	MLIST	lists.apache.org

#102197: Security Vulnerabilities in the Apache 1.3 Web Server	SUNALERT	sunsolve.sun.com
Secunia - Advisories - Avaya Products httpd/mod_ssl Vulnerabilities	SECUNIA	secunia.com
US-CERT Vulnerability Note VU#744929	CERT-VN	www.kb.cert.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP server 2.0.55: http://httpd.apache.org/security/vulnerabilities_20.html

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 registred 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.

CVE.report and Source URL Uptime Status status.cve.report