



CVE-2004-0700

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

Summary

CVE	CVE-2004-0700
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-07-27 04:00:00 UTC
Updated	2017-07-11 01:30:00 UTC
Description	Format string vulnerability in the mod_proxy hook functions function in ssl_engine_log.c in mod_ssl before 2.8.19 for Apache

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Application	Mod Ssl	Mod Ssl	2.3.11	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.10	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.3	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.4	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.5	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.7	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.9	All	All	All
Application	Mod Ssl	Mod Ssl	2.5.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.5.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.0	All	All	All

Application	Mod Ssl	Mod Ssl	2.6.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.3	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.4	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.5	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.7.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.7.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.1.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.10	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.12	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	2.8.17	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.18	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.3	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.4	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.5	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.5.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.5.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.7	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.9	All	All	All
Application	Mod Ssl	Mod Ssl	2.3.11	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.10	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.3	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.4	All	All	All

Application	Mod Ssl	Mod Ssl	2.4.5	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.7	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.4.9	All	All	All
Application	Mod Ssl	Mod Ssl	2.5.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.5.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.3	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.4	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.5	All	All	All
Application	Mod Ssl	Mod Ssl	2.6.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.7.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.7.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.0	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.1.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.10	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.12	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	2.8.17	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.18	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.3	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.4	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.5	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.5.1	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.5.2	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.6	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.7	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.8	All	All	All
Application	Mod Ssl	Mod Ssl	2.8.9	All	All	All

Application	Mod Ssl	Mod Ssl	2.8.9	All	All	All
References						
Reference	Source	Link	Tags			
redhat.com Red Hat Support	REDHAT	www.redhat.com				
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com				
Files ≈ Packet Storm	MISC	packetstormsecurity.org				
redhat.com Red Hat Support	REDHAT	www.redhat.com				
usn/usn-177-1 - Ubuntu Linux	UBUNTU	www.ubuntu.com				
virulent.siyahsapka.org	MISC	virulent.siyahsapka.org				
MDKSA-2004:075	MANDRAKE	www.mandrakesecure.net				
Apache 'mod_ssl' Log Function Format String Vulnerability	BID	www.securityfocus.com				
Home - Conectiva	CONNECTIVA	distro.conectiva.com.br				
7929	OSVDB	www.osvdb.org				
'[ANNOUNCE] mod_ssl 2.8.19 for Apache 1.3.31' - MARC	MLIST	marc.info				
'[OpenPKG-SA-2004.032] OpenPKG Security Advisory (apache)' - MARC	BUGTRAQ	marc.info				
US-CERT Vulnerability Note VU#303448	CERT-VN	www.kb.cert.org	Third Party Adv			
FLSA:1888	FEDORA	bugzilla.fedora.us				
Debian -- Security Information -- DSA-532-2 libapache-mod-ssl	DEBIAN	www.debian.org				
CVE Program record	CVE.ORG	www.cve.org	canonical			
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy			

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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

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