



CVE-2009-0591

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

Summary

CVE	CVE-2009-0591
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-27 16:30:00 UTC
Updated	2017-08-17 01:29:00 UTC
Description	The CMS_verify function in OpenSSL 0.9.8h through 0.9.8j, when CMS is enabled, does not properly handle errors associa

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All
Application	Openssl	Openssl	0.9.8h	All	All	All
Application	Openssl	Openssl	0.9.8i	All	All	All
Application	Openssl	Openssl	0.9.8j	All	All	All

References

Reference	Source
kb.bluecoat.com/index	CONFIRM
VooDoo cIRClE download SourceForge.net	CONFIRM
OpenSSL Multiple Vulnerabilities	BID
About Secunia Research Flexera	SECUNIA
OpenSSL CMS_verify() Error Handling Flaw Lets Users Bypass Security Checks - SecurityTracker	SECTrack
NetBSD-SA2009-008	NETBSD
About Security Update 2009-005	CONFIRM
PHP for Windows OpenSSL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA

[security-announce] SUSE Security Summary Report: SUSE-SR:2009:010	SUSE
About Secunia Research Flexera	SECUNIA
Webmail OVH- OVH	VUPEN
APPLE-SA-2009-09-10-2 Security Update 2009-005	APPLE
VooDoo cIRcLe security advisory 20090326-01	CONFIRM
OpenSSL Multiple Vulnerabilities - Advisories - Community	SECUNIA
NetBSD update for openssl - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
SSRT090059	HP
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Webmail - OVH	VUPEN
52865	OSVDB
SUSE Update for Multiple Packages - Advisories - Community	SECUNIA
VooDoo cIRcLe OpenSSL Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
www.openssl.org/news/secadv_20090325.txt	CONFIRM
Webmail - OVH	VUPEN
HP-UX update for OpenSSL - Secunia.com	SECUNIA
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
PHP: News Archive - 2009	CONFIRM
'[security bulletin] HPSBOV02540 SSRT090249 rev.1 - HP SSL for OpenVMS, Remote Unauthorized Data Inje' - MARC	HP
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-03-30	Tomas Hoger	Not vulnerable. This issue affected OpenSSL CMS functionality which is not present in the ope

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

