



CVE-2011-0014

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

Summary

CVE	CVE-2011-0014
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-19 01:00:00 UTC
Updated	2017-09-19 01:31:00 UTC
Description	ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service

Risk And Classification

Problem Types: CWE-399

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	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8q	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All

Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	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
Application	Openssl	Openssl	0.9.8k	All	All	All
Application	Openssl	Openssl	0.9.8l	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8q	All	All	All
Application	Openssl	Openssl	1.0.0	All	All	All
Application	Openssl	Openssl	1.0.0	beta1	All	All
Application	Openssl	Openssl	1.0.0	beta2	All	All
Application	Openssl	Openssl	1.0.0	beta3	All	All
Application	Openssl	Openssl	1.0.0	beta4	All	All
Application	Openssl	Openssl	1.0.0	beta5	All	All
Application	Openssl	Openssl	1.0.0a	All	All	All
Application	Openssl	Openssl	1.0.0b	All	All	All
Application	Openssl	Openssl	1.0.0c	All	All	All

References

Reference	Source	Link
Security Advisory SA57353 - IBM Storage System DS8870 OpenSSL Multiple Vulnerabilities - Secunia	SECUNIA	see
APPLE-SA-2011-06-23-1 Mac OS X v10.6.8 and Security Update 2011-004	APPLE	list
IBM Security Bulletin: Storage HMC OpenSSL upgrade to address cryptographic vulnerabilities. - United States	CONFIRM	ww
HPSBMA02658	HP	h2
HP Insight Control for Linux Multiple Vulnerabilities - Secunia.com	SECUNIA	see
OpenSSL ClientHello Handshake Message Parsing Vulnerability - Secunia.com	SECUNIA	see
70847	OSVDB	os
OpenSSL ClientHello Parsing Flaw Lets Remote Users Deny Service - SecurityTracker	SECTRACK	ww
Support	REDHAT	ww
[SECURITY] Fedora 14 Update: openssl-1.0.0d-1.fc14	FEDORA	list
USN-1064-1: OpenSSL vulnerability Ubuntu	UBUNTU	ww
Multiple CVEs in OpenSSL - CVE Details	MUSEM	

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
www.openssl.org/news/secadv_20110208.txt	CONFIRM	ww
Repository / Oval Repository	OVAL	ov:
Slackware update for openssl - Secunia.com	SECUNIA	se
support.f5.com/csp/article/K10534046	CONFIRM	su
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	sla
Fedora update for openssl - Secunia.com	SECUNIA	se
NetBSD-SA2011-002	NETBSD	ftp
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Debian update for openssl - Secunia.com	SECUNIA	se
About the security content of Mac OS X v10.6.8 and Security Update 2011-004 - Apple Support	CONFIRM	su
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Security Advisories Mandriva Linux	MANDRIVA	ww
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
Debian -- Security Information -- DSA-2162-1 openssl	DEBIAN	ww
OpenSSL OCSP Stapling 'ClientHello' Handshake Message Parsing Security Vulnerability	BID	ww
'[security bulletin] HPSBUX02689 SSRT100494 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC	HP	me
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:005	SUSE	list
'[security bulletin] HPSBOV02670 SSRT100475 rev.1 - HP OpenVMS running SSL, Remote Denial of Service' - MARC	HP	me
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[390226](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2021-0011)

[390284](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Open Secure Sockets Layer (OpenSSL) (OVMSA-2023-0013)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)