



CVE-2011-3207

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

Summary

CVE	CVE-2011-3207
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-22 10:55:00 UTC
Updated	2014-03-26 04:22:00 UTC
Description	crypto/x509/x509_vfy.c in OpenSSL 1.0.x before 1.0.0e does not initialize certain structure members, which makes it easier

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	1.0.0d	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	1.0.0d	All	All	All

References

Reference	Source
Security Advisory SA57353 - IBM Storage System DS8870 OpenSSL Multiple Vulnerabilities - Secunia	SECUN
IBM Security Bulletin: Storage HMC OpenSSL upgrade to address cryptographic vulnerabilities. - United States	CONFIF
Bug 736087 – CVE-2011-3207 openssl: CRL verification vulnerability	CONFIF
openssl.org/news/secadv_20110906.txt	CONFIF
[SECURITY] Fedora 18 Update: mingw-openssl-1.0.1c-1.fc18	FEDOR
[SECURITY] Fedora 16 Update: openssl-1.0.0e-1.fc16	FEDOR
[security bulletin] HPSBMU02752 SSRT100802 rev.1 HP Insight Control Software for Linux (IC-Linux), R' - MARC	HP
Support	REDHA
[SECURITY] Fedora 14 Update: openssl-1.0.0e-1.fc14	FEDOR
Fedora update for openssl - Secunia.com	SECUN
APPLE-SA-2013-06-04-1 OS X Mountain Lion v10.8.4 and Security Update 2013-002	APPLE
OpenSSL ECDH Ciphersuite and CRL Update Bugs Lets Remote Users Deny Service and Bypass CRL Updates - SecurityTracker	SECTR
Support / Security / Advisories // MDVSA-2011:137 Mandriva	MANDF
cvs.openssl.org/chngview	CONFIF
About the security content of OS X Mountain Lion v10.8.4 and Security Update 2013-002	CONFIF
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

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](#)