CVE-2015-0209

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-0209
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-19 22:59:00 UTC
Updated	2023-11-07 02:23:00 UTC
Description	Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 befor

Risk And Classification

Problem Types: NVD-CWE-Other

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	1.0.0a	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	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	All	All
Application	Openssl	Openssl	1.0.0p	All	All	All

Application	Openssl	Openssl	1.0.0q	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All
Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	1.0.0	All	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	1.0.0e	All	All	All
Application	Openssl	Openssl	1.0.0f	All	All	All
Application	Openssl	Openssl	1.0.0g	All	All	All
Application	Openssl	Openssl	1.0.0h	All	All	All
Application	Openssl	Openssl	1.0.0i	All	All	All
Application	Openssl	Openssl	1.0.0j	All	All	All
Application	Openssl	Openssl	1.0.0k	All	All	All
Application	Openssl	Openssl	1.0.0l	All	All	All
Application	Openssl	Openssl	1.0.0m	All	All	All
Application	Openssl	Openssl	1.0.0n	All	All	All
Application	Openssl	Openssl	1.0.0o	All	All	All
Application	Openssl	Openssl	1.0.0p	All	All	All
Application	Openssl	Openssl	1.0.0q	All	All	All
Application	Openssl	Openssl	1.0.1	All	All	All

Application	Openssl	Openssl	1.0.1a	All	All	All
Application	Openssl	Openssl	1.0.1b	All	All	All
Application	Openssl	Openssl	1.0.1c	All	All	All
Application	Openssl	Openssl	1.0.1d	All	All	All
Application	Openssl	Openssl	1.0.1e	All	All	All
Application	Openssl	Openssl	1.0.1f	All	All	All
Application	Openssl	Openssl	1.0.1g	All	All	All
Application	Openssl	Openssl	1.0.1h	All	All	All
Application	Openssl	Openssl	1.0.1i	All	All	All
Application	Openssl	Openssl	1.0.1j	All	All	All
Application	Openssl	Openssl	1.0.1k	All	All	All
Application	Openssl	Openssl	1.0.1l	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All

References

Reference	Source	L
Red Hat Customer Portal	REDHAT	rh
About the security content of OS X Yosemite v10.10.4 and Security Update 2015-005 - Apple Support	CONFIRM	su
Oracle Bulletin Board Update - January 2015	CONFIRM	w
OpenSSL CVE-2015-0209 Remote Memory Corruption Vulnerability	BID	w
openSUSE-SU-2015:0554-1: moderate: Security update for openssl	SUSE	lis
FreeBSD-SA-15:06	FREEBSD	w
Red Hat Customer Portal	REDHAT	rh
Oracle Critical Patch Update - October 2015	CONFIRM	w
Multiple Security Vulnerabilities in Citrix NetScaler Platform IPMI Lights Out Management (LOM) firmware	CONFIRM	su
Gentoo Security	GENTOO	se
Oracle Critical Patch Update - July 2015	CONFIRM	w
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC	HP	m
git.openssl.org Git - openssl.git/commit	CONFIRM	gi
APPLE-SA-2015-06-30-2 OS X Yosemite v10.10.4 and Security Update 2015-005	APPLE	lis
www.openssl.org/news/secadv_20150319.txt	CONFIRM	w
'[security bulletin] HPSBMU03397 rev.1 - HP Version Control Agent (VCA) on Windows and Linux, Multipl' - MARC	HP	m
Support / Security / Advisories / / MDVSA-2015:062 | Mandriva	MANDRIVA	w
Support / Security / Advisories / / MDVSA-2015:063 | Mandriva	MANDRIVA	w
git.openssl.org Git - openssl.git/commit		gi
RHSA-2016:1089	REDHAT	rh

[security-announce] SUSE-SU-2015:0541-1: important: Security update for	SUSE	lis
[SECURITY] Fedora 22 Update: openssl-1.0.1k-6.fc22	FEDORA	lis
[SECURITY] Fedora 20 Update: openssl-1.0.1e-42.fc20	FEDORA	lis
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	ce
OpenSSL Multiple Flaws Let Remote Users Deny Service - SecurityTracker	SECTRACK	w
'[security bulletin] HPSBUX03334 SSRT102000 rev.1 - HP-UX Running OpenSSL, Remote Denial of Service (' - MARC	HP	m
[SECURITY] Fedora 21 Update: mingw-openssl-1.0.2a-1.fc21	FEDORA	lis
USN-2537-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	w
2015-04 Security Bulletin: OpenSSL 19th March 2015 advisory - Juniper Networks	CONFIRM	kb
OpenSSL Updates of 19 March 2015 - Red Hat Customer Portal	CONFIRM	ac
[security-announce] openSUSE-SU-2015:1277-1: important: Security update	SUSE	lis
1196737 – (CVE-2015-0209) CVE-2015-0209 openssl: use-after-free on invalid EC private key import	CONFIRM	bu
[security-announce] openSUSE-SU-2016:0640-1: important: Security update	SUSE	lis
[SECURITY] Fedora 21 Update: openssl-1.0.1k-6.fc21	FEDORA	lis
'[security bulletin] HPSBMU03380 rev.1 - HP System Management Homepage (SMH) on Linux and Windows, Mu' - MARC	HP	m
[SECURITY] Fedora 22 Update: mingw-openssl-1.0.2a-1.fc22	FEDORA	lis
'[security bulletin] HPSBMU03413 rev.1 - HP Virtual Connect Enterprise Manager SDK, Multiple Vulnerab' - MARC	HP	m
Red Hat Customer Portal	REDHAT	rh
Oracle Solaris Third Party Bulletin - April 2015	CONFIRM	w
Broadcom Support Portal	CONFIRM	bt
Debian -- Security Information -- DSA-3197-1 openssl	DEBIAN	w
Oracle Critical Patch Update - October 2017	CONFIRM	w
'[security bulletin] HPSBGN03306 rev.1 - HP IceWall SSO MCRP, SSO Dfw, and SSO Agent running OpenSSL,' - MARC	HP	m
Red Hat Customer Portal	REDHAT	rh
McAfee KnowledgeBase - Intel Security - Security Bulletin: Fourteen OpenSSL CVEs Announced on March 19, 2015	CONFIRM	kc
Oracle Critical Patch Update - January 2016	CONFIRM	w
CVE Program record	CVE.ORG	w
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)

590349 Rockwell Automation Stratix 5900 Multiple Vulnerabilities (ICSA-17-094-04)

591280 Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672)