CVE-2015-0292

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-0292
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	Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in Op

Risk And Classification

Problem Types: CWE-119

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	1.0.1	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	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	1.0.1	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

References

Reference	Source	L
Red Hat Customer Portal	REDHAT	rh
Oracle Bulletin Board Update - January 2015	CONFIRM	w
Red Hat Customer Portal	REDHAT	rh
git.openssl.org Git - openssl.git/commit	CONFIRM	gi
FortiGuard	CONFIRM	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
git.openssl.org Git - openssl.git/commit		gi
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC	HP	m
[security-announce] SUSE-SU-2015:0578-1: important: Security update for	SUSE	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
#2608: bug report: segfault from base64 decoding	CONFIRM	rt
[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
USN-2537-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	w
1202395 – (CVE-2015-0292) CVE-2015-0292 openssl: integer underflow leading to buffer overflow in base64 decoding	CONFIRM	bu
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] 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
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
OpenSSL '/evp/encode.c' Remote Memory Corruption Vulnerability	BID	w
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)

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