CVE-2015-3193

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3193
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-06 20:59:00 UTC
Updated	2023-02-13 00:47:00 UTC
Description	The Montgomery squaring implementation in crypto/bn/asm/x86_64-mont5.pl in OpenSSL 1.0.2 before 1.0.2e on the x86_6

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2a	All	All	All
Application	Openssl	Openssl	1.0.2b	All	All	All
Application	Openssl	Openssl	1.0.2c	All	All	All
Application	Openssl	Openssl	1.0.2d	All	All	All

References

Reference	Source	Li
Oracle Critical Patch Update Advisory - April 2016	CONFIRM	wv
USN-2830-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	wv
404 Page not found	CONFIRM	kb
Multiple Vulnerabilities in OpenSSL (December 2015) Affecting Cisco Products	CISCO	toc
Oracle Critical Patch Update - July 2016	CONFIRM	wv
openssl.org/news/secadv/20151203.txt	CONFIRM	op
git.openssl.org Git - openssl.git/commit	MISC	git
Oracle July 2016 Critical Patch Update Multiple Vulnerabilities	BID	wv
git.openssl.org Git - openssl.git/commit	CONFIRM	git
Malformed Request	BID	wv
FortiGuard.com | OpenSSL Advisory - December 2015	CONFIRM	for
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	wv
Fuzzing Math - miscalculations in OpenSSL's BN_mod_exp (CVE-2015-3193) | The Fuzzing Project	MISC	blo
Bug 1288317 – CVE-2015-3193 OpenSSL: BN_mod_exp may produce incorrect results on x86_64	CONFIRM	bu
Public KB - SA40100 - [Pulse Secure] December 3rd 2015 OpenSSL Security Advisory	CONFIRM	kb
2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks	CONFIRM	kb
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	ce
Document Display | HPE Support Center	CONFIRM	h2
FortiGuard.com | OpenSSL Advisory - December 2015	CONFIRM	wv
Juniper Networks - 2016-10 Security Bulletin: OpenSSL security updates	CONFIRM	kb
OpenSSL Multiple Bugs Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK	wv
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE	wv
Oracle Critical Patch Update - October 2017	CONFIRM	wv
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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