CVE-2015-1794

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-1794
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 00:46:00 UTC
Description	The ssl3_get_key_exchange function in ssl/s3_clnt.c in OpenSSL 1.0.2 before 1.0.2e allows remote servers to cause a den

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	ww
USN-2830-1: OpenSSL vulnerabilities | Ubuntu	UBUNTU	ww
Multiple Vulnerabilities in OpenSSL (December 2015) Affecting Cisco Products	CISCO	toc
[security-announce] openSUSE-SU-2016:0637-1: important: Security update	SUSE	list

openssl.org/news/secadv/20151203.txt	CONFIRM	op
FortiGuard.com | OpenSSL Advisory - December 2015	CONFIRM	for
git.openssl.org Git - openssl.git/commit	CONFIRM	git
2016-10 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks	CONFIRM	kb
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	ce
git.openssl.org Git - openssl.git/commit	MISC	git
Document Display | HPE Support Center	CONFIRM	h2
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
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)