CVE-2015-0285

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-0285
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	The ssl3_client_hello function in s3_clnt.c in OpenSSL 1.0.2 before 1.0.2a does not ensure that the PRNG is seeded before

Risk And Classification

Problem Types: CWE-310

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	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All
Application	Openssl	Openssl	1.0.2	All	All	All
Application	Openssl	Openssl	1.0.2	beta1	All	All
Application	Openssl	Openssl	1.0.2	beta2	All	All
Application	Openssl	Openssl	1.0.2	beta3	All	All

References

Reference	Source	L
1202410 – (CVE-2015-0285) CVE-2015-0285 openssl: handshake with unseeded PRNG	CONFIRM	b
git.openssl.org Git - openssl.git/commit		g
FortiGuard	CONFIRM	w
Oracle Critical Patch Update - October 2015	CONFIRM	w
Gentoo Security	GENTOO	s
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
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
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	ce
OpenSSL CVE-2015-0285 Insufficient Entropy Security Weakness	BID	w
OpenSSL Multiple Flaws Let Remote Users Deny Service - SecurityTracker	SECTRACK	w
'[security bulletin] HPSBMU03380 rev.1 - HP System Management Homepage (SMH) on Linux and Windows, Mu' - MARC	HP	m
Oracle Solaris Third Party Bulletin - April 2015	CONFIRM	w
Broadcom Support Portal	CONFIRM	bt
Oracle Critical Patch Update - October 2017	CONFIRM	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

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)