CVE-2015-3216

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3216
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-07 10:59:00 UTC
Updated	2018-01-05 02:30:00 UTC
Description	Race condition in a certain Red Hat patch to the PRNG lock implementation in the ssleay_rand_bytes function in OpenSSL

Risk And Classification

Problem Types: CWE-189 | CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	1.0.1e-25.el7	All	All	All
Application	Openssl	Openssl	1.0.1e-25.el7	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source	Link
Red Hat OpenSSL Locking Error in ssleay_rand_bytes() Lets Remote Users Deny Service - SecurityTracker	SECTRACK	www.securitytra
[security-announce] SUSE-SU-2015:1143-1: important: Security update for	SUSE	lists.opensuse.c
[security-announce] SUSE-SU-2015:1182-1: important: Security update for	SUSE	lists.opensuse.c
[security-announce] SUSE-SU-2015:1184-1: important: Security update for	SUSE	lists.opensuse.c
[security-announce] SUSE-SU-2015:1150-1: important: Security update for	SUSE	lists.opensuse.c
Red Hat Customer Portal	REDHAT	rhn.redhat.com
OpenSSL 'ssleay_rand_bytes()' Function Denial of Service Vulnerability	BID	www.securityfoc
Red Hat Customer Portal	REDHAT	rhn.redhat.com
Bug 1225994 – segfault in ssleay_rand_bytes due to locking regression	CONFIRM	bugzilla.redhat.c
[security-announce] openSUSE-SU-2015:1139-1: important: Security update	SUSE	lists.opensuse.c

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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)