CVE-2014-0017

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-0017
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-14 15:55:00 UTC
Updated	2014-03-26 04:55:00 UTC
Description	The RAND_bytes function in libssh before 0.6.3, when forking is enabled, does not properly reset the state of the OpenSSL

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libssh	Libssh	0.4.7	All	All	All
Application	Libssh	Libssh	0.4.8	All	All	All
Application	Libssh	Libssh	0.5.0	All	All	All
Application	Libssh	Libssh	0.5.0	rc1	All	All
Application	Libssh	Libssh	0.5.1	All	All	All
Application	Libssh	Libssh	0.5.2	All	All	All
Application	Libssh	Libssh	0.5.3	All	All	All
Application	Libssh	Libssh	0.5.4	All	All	All
Application	Libssh	Libssh	0.5.5	All	All	All
Application	Libssh	Libssh	0.6.0	All	All	All
Application	Libssh	Libssh	0.6.1	All	All	All
Application	Libssh	Libssh	All	All	All	All
Application	Libssh	Libssh	0.4.7	All	All	All
Application	Libssh	Libssh	0.4.8	All	All	All
Application	Libssh	Libssh	0.5.0	All	All	All
Application	Libssh	Libssh	0.5.0	rc1	All	All
Application	Libssh	Libssh	0.5.1	All	All	All

Application	Libssh	Libssh	0.5.2	All	All	All
Application	Libssh	Libssh	0.5.3	All	All	All
Application	Libssh	Libssh	0.5.4	All	All	All
Application	Libssh	Libssh	0.5.5	All	All	All
Application	Libssh	Libssh	0.6.0	All	All	All
Application	Libssh	Libssh	0.6.1	All	All	All

References

Reference	Source	Link	Tags
USN-2145-1: libssh vulnerability | Ubuntu	UBUNTU	www.ubuntu.com	
Debian -- Security Information -- DSA-2879-1 libssh	DEBIAN	www.debian.org	
libssh 0.6.3 (Security release) at libssh - The SSH Library!	CONFIRM	www.libssh.org	Patch, Vendor Adviso
Security Advisory SA57407 - Ubuntu update for libssh - Secunia	SECUNIA	secunia.com	Vendor Advisory
Bug 1072191 – CVE-2014-0017 libssh: Improper initialization of PRNG after fork()	CONFIRM	bugzilla.redhat.com	
openSUSE-SU-2014:0366-1: moderate: libssh: reseed randomness on forking	SUSE	lists.opensuse.org	
openSUSE-SU-2014:0370-1: moderate: libssh: reseed randomness on forking	SUSE	lists.opensuse.org	
oss-security - libssh and stunnel PRNG flaws	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.