CVE-2013-0176

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-0176
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-05 23:55:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	The publickey_from_privatekey function in libssh before 0.5.4, when no algorithm is matched during negotiations, allows rei

Risk And Classification

Problem Types: CWE-399

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	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

References

Reference	Source	Link	Tags
Security Advisory SA51982 - Ubuntu update for libssh - Secunia	SECUNIA	secunia.com	Vendor Advisory

libssh 0.5.4 (SECURITY RELEASE) at libssh - The SSH Library!	CONFIRM	www.libssh.org	Patch, Vendor Advisory
[SECURITY] Fedora 17 Update: libssh-0.5.4-1.fc17	FEDORA	lists.fedoraproject.org	
USN-1707-1: libssh vulnerability | Ubuntu	UBUNTU	www.ubuntu.com	
[SECURITY] Fedora 18 Update: libssh-0.5.4-1.fc18	FEDORA	lists.fedoraproject.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.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.