



# CVE-2014-8132

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2014-8132
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-12-29 00:59:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	Double free vulnerability in the ssh_packet_kexinit function in kex.c in libssh 0.5.x and 0.6.x before 0.6.4 allows remote atta

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	19	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	19	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	20	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	21	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.0	All	All	All

Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.2	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.3	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.4	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.5	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.0	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.1	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.2	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.3	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.0	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.2	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.3	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.4	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.5.5	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.0	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.1	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.2	All	All	All
Application	<a href="#">Libssh</a>	<a href="#">Libssh</a>	0.6.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.2	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 19 Update: libssh-0.6.4-1.fc19	FEDORA	<a href="#">lists.fedoraproje</a>
Debian -- Security Information -- DSA-3488-1 libssh	DEBIAN	<a href="#">www.debian.org</a>
Support / Security / Advisories // MDVSA-2015:020   Mandriva	MANDRIVA	<a href="#">www.mandriva.</a>
openSUSE-SU-2015:0017-1: moderate: Security update for libssh	SUSE	<a href="#">lists.opensuse.c</a>
[SECURITY] Fedora 21 Update: libssh-0.6.4-1.fc21	FEDORA	<a href="#">lists.fedoraproje</a>
libssh 0.6.4 (Security and bugfix release) at libssh - The SSH Library!	CONFIRM	<a href="#">www.libssh.org</a>
[SECURITY] Fedora 20 Update: libssh-0.6.4-1.fc20	FEDORA	<a href="#">lists.fedoraproje</a>
Security Advisory SA60838 - SUSE update for libssh - Secunia	SECUNIA	<a href="#">secunia.com</a>
Bug 1158089 – CVE-2014-8132 libssh: Possible double free on a dangling pointer with crafted kexinit packet	CONFIRM	<a href="#">bugzilla.redhat.</a>
libssh 0.6.4 (Security and bugfix release) at libssh - The SSH Library!	CONFIRM	<a href="#">www.libssh.org</a>

libssh and libssh2: Multiple vulnerabilities (GLSA 201606-12) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo</a>
Mageia Advisory: MGASA-2015-0014 - Updated libssh packages fix CVE-2014-8132	CONFIRM	<a href="http://advisories.mageia.org">advisories.mageia.org</a>
USN-2478-1: libssh vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](http://CVE.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)