



# CVE-2019-3860

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

## Summary

<b>CVE</b>	CVE-2019-3860
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-25 19:29:00 UTC
<b>Updated</b>	2023-11-07 03:10:00 UTC
<b>Description</b>	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parse

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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>	8.0	All	All	All
Application	<a href="#">Libssh2</a>	<a href="#">Libssh2</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update	BUGTRAQ	<a href="#">seclists.org</a>
[security-announce] openSUSE-SU-2019:1640-1: moderate: Security update f	SUSE	<a href="#">lists.opensuse.org</a>
March 2019 Libssh2 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
Debian -- Security Information -- DSA-4431-1 libssh2	DEBIAN	<a href="#">www.debian.org</a>

[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.org</a>
[security-announce] openSUSE-SU-2019:1075-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org/">lists.opensuse.org</a>
libssh2 Security Advisory: CVE-2019-3860	MISC	<a href="http://www.libssh2.org/">www.libssh2.org</a>
1687310 – (CVE-2019-3860) CVE-2019-3860 libssh2: Out-of-bounds reads with specially crafted SFTP packets	CONFIRM	<a href="https://bugzilla.redhat.com/">bugzilla.redhat.com</a>
[SECURITY] [DLA 1730-1] libssh2 security update	MLIST	<a href="https://lists.debian.org/">lists.debian.org</a>
Oracle Critical Patch Update - October 2019	MISC	<a href="http://www.oracle.com/">www.oracle.com</a>
[security-announce] openSUSE-SU-2019:1109-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org/">lists.opensuse.org</a>
[SECURITY] [DLA 1730-4] libssh2 regression update	MLIST	<a href="https://lists.debian.org/">lists.debian.org</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.

#### Legacy QID Mappings

- [355094](#) Amazon Linux Security Advisory for libssh2 : ALAS2-2023-2046
- [355347](#) Amazon Linux Security Advisory for libssh2 : ALAS-2023-1756
- [355524](#) Amazon Linux Security Advisory for libssh2 : AL2012-2023-423
- [500318](#) Alpine Linux Security Update for libssh2
- [504085](#) Alpine Linux Security Update for libssh2
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- [750528](#) OpenSUSE Security Update for libssh2\_org (openSUSE-SU-2020:2129-1)
- [750530](#) OpenSUSE Security Update for libssh2\_org (openSUSE-SU-2020:2126-1)

© [CVE.report](https://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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

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