



# CVE-2019-3855

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-3855
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-21 21:29:00 UTC
<b>Updated</b>	2023-11-07 03:10:00 UTC
<b>Description</b>	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packe

## Risk And Classification

**Problem Types:** CWE-787 | CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apple</a>	<a href="#">Xcode</a>	All	All	All	All
Application	<a href="#">Apple</a>	<a href="#">Xcode</a>	All	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>	9.0	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>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	28	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Application	<a href="#">Libssh2</a>	<a href="#">Libssh2</a>	All	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>	42.3	All	All	All

Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.56	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.57	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.56	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Peoplesoft Enterprise Peopletools</a>	8.57	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
[SECURITY] Fedora 29 Update: libssh2-1.9.0-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fe</a>
Broadcom Inc.   Connecting Everything	CONFIRM	<a href="#">www.l</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
[SECURITY] Fedora 30 Update: libssh2-1.9.0-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update	BUGTRAQ	<a href="#">seclis</a>
Red Hat Customer Portal	REDHAT	<a href="#">access</a>
oss-security - [SECURITY ADVISORIES] libssh2	MLIST	<a href="#">www.l</a>
March 2019 Libssh2 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">secur</a>
Debian -- Security Information -- DSA-4431-1 libssh2	DEBIAN	<a href="#">www.l</a>
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fe</a>
[SECURITY] Fedora 29 Update: libssh2-1.8.1-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fe</a>

libssh2 Security Advisory: CVE-2019-3855	MISC	<a href="#">www.i</a>
[security-announce] openSUSE-SU-2019:1075-1: moderate: Security update f	SUSE	<a href="#">lists.o</a>
Slackware Security Advisory - libssh2 Updates ≈ Packet Storm	MISC	<a href="#">packe</a>
About the security content of Xcode 11.0 - Apple Support	CONFIRM	<a href="#">suppc</a>
Red Hat Customer Portal	REDHAT	<a href="#">acces</a>
[SECURITY] [DLA 1730-1] libssh2 security update	MLIST	<a href="#">lists.d</a>
libssh2 Multiple Security Vulnerabilities	BID	<a href="#">www.:</a>
Full Disclosure: APPLE-SA-2019-9-26-7 Xcode 11.0	FULLDISC	<a href="#">seclis</a>
[SECURITY] Fedora 29 Update: libssh2-1.8.1-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
[SECURITY] Fedora 30 Update: libssh2-1.9.0-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fe</a>
Red Hat Customer Portal	REDHAT	<a href="#">acces</a>
Bugtraq: APPLE-SA-2019-9-26-7 Xcode 11.0	BUGTRAQ	<a href="#">seclis</a>
Oracle Critical Patch Update - October 2019	MISC	<a href="#">www.:</a>
[security-announce] openSUSE-SU-2019:1109-1: moderate: Security update f	SUSE	<a href="#">lists.o</a>
1687303 – (CVE-2019-3855) CVE-2019-3855 libssh2: Integer overflow in transport read resulting in out of bounds write	CONFIRM	<a href="#">bugzil</a>
[SECURITY] Fedora 29 Update: libssh2-1.9.0-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
Red Hat Customer Portal	REDHAT	<a href="#">acces</a>
Bugtraq: [slackware-security] libssh2 (SSA:2019-077-01)	BUGTRAQ	<a href="#">seclis</a>
CVE Program record	CVE.ORG	<a href="#">www.:</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)
- [377077](#) Alibaba Cloud Linux Security Update for libssh2 (ALINUX2-SA-2019:0018)
- [378237](#) Virtuozzo Linux Security Update for libssh2-docs (VZLSA-2019:1652)
- [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](#) 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**