



CVE-2019-3856

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

Summary

CVE	CVE-2019-3856
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-25 19:29:00 UTC
Updated	2023-11-07 03:10:00 UTC
Description	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyb

Risk And Classification

Problem Types: CWE-787 | CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Application	Libssh2	Libssh2	All	All	All	All
Application	Libssh2	Libssh2	All	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.56	All	All	All

Application	Oracle	Peoplesoft Enterprise Peopletools	8.57	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source
Red Hat Customer Portal	RED
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	
Red Hat Customer Portal	RED
Bugtraq: [SECURITY] [DSA 4431-1] libssh2 security update	BUG
Red Hat Customer Portal	RED
March 2019 Libssh2 Vulnerabilities in NetApp Products NetApp Product Security	COI
Debian -- Security Information -- DSA-4431-1 libssh2	DEE
[SECURITY] Fedora 28 Update: libssh2-1.8.1-1.fc28 - package-announce - Fedora Mailing-Lists	FED
[security-announce] openSUSE-SU-2019:1075-1: moderate: Security update f	SUS
libssh2 Security Advisory: CVE-2019-3856	MIS
Red Hat Customer Portal	RED
1687304 – (CVE-2019-3856) CVE-2019-3856 libssh2: Integer overflow in keyboard interactive handling resulting in out of bounds write	COI
[SECURITY] [DLA 1730-1] libssh2 security update	MLI
Red Hat Customer Portal	RED
Oracle Critical Patch Update - October 2019	MIS
[security-announce] openSUSE-SU-2019:1109-1: moderate: Security update f	SUS
Red Hat Customer Portal	RED

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[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](#)