



CVE-2019-17498

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-17498
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-21 22:15:00 UTC
Updated	2023-11-07 03:06:00 UTC
Description	In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds c

Risk And Classification

Problem Types: 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	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Libssh2	Libssh2	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Operating System	Netapp	Bootstrap Os	-	All	All	All
Application	Netapp	Element Software	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 31 Update: libssh2-1.9.0-3.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	TR
packet.c: improve message parsing (#402) · libssh2/libssh2@dedcbd1 · GitHub	MISC	github.com	Pa
CVE-2019-17498 Libssh2 Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
libssh2/packet.c at 42d37aa63129a1b2644bf6495198923534322d64 · libssh2/libssh2 · GitHub	MISC	github.com	Ex
[SECURITY] Fedora 30 Update: libssh2-1.9.0-3.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	TR
libssh2 1.9.0 Out-Of-Bounds Read ≈ Packet Storm	MISC	packetstormsecurity.com	
[security-announce] openSUSE-SU-2019:2483-1: moderate: Security update f	SUSE	lists.opensuse.org	TR
[SECURITY] [DLA 1991-1] libssh2 security update	MLIST	lists.debian.org	TR
[SECURITY] Fedora 30 Update: libssh2-1.9.0-3.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Another libssh2 integer overflow (CVE-2019-17498) Semmler Blog	MISC	blog.semmler.com	Ex
[SECURITY] Fedora 31 Update: libssh2-1.9.0-3.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Page not found · GitHub · GitHub	MISC	github.com	Ex
[SECURITY] [DLA 2848-1] libssh2 security update	MLIST	lists.debian.org	
[SECURITY] [DLA 3559-1] libssh2 security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [178944](#) Debian Security Update for libssh2 (DLA 2848-1)
- [296075](#) Oracle Solaris 11.4 Support Repository Update (SRU) 21.69.0 Missing (CPUAPR2020)
- [377296](#) Alibaba Cloud Linux Security Update for libssh2 (ALINUX2-SA-2020:0132)
- [500320](#) Alpine Linux Security Update for libssh2
- [504087](#) Alpine Linux Security Update for libssh2
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- [6000057](#) Debian Security Update for libssh2 (DLA 3559-1)
- [750528](#) OpenSUSE Security Update for libssh2_org (openSUSE-SU-2020:2129-1)
- [750530](#) OpenSUSE Security Update for libssh2_org (openSUSE-SU-2020:2126-1)
- [900070](#) CBL-Mariner Linux Security Update for libssh2 1.9.0

900965 Common Base Linux Mariner (CBL-Mariner) Security Update for libssh2 (6650-1)

903013 Common Base Linux Mariner (CBL-Mariner) Security Update for libssh2 (1819)

© [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](#)