



CVE-2020-22218

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

Summary

CVE	CVE-2020-22218
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-22 19:16:00 UTC
Updated	2023-10-06 15:15:00 UTC
Description	An issue was discovered in function <code>_libssh2_packet_add</code> in <code>libssh2 1.10.0</code> allows attackers to access out of bounds memo

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libssh2	Libssh2	1.10.0	All	All	All

References

Reference	Source	Link	Tags
CVE-2020-22218 Libssh2 Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] [DLA 3559-1] libssh2 security update	MLIST	lists.debian.org	
fix use-of-uninitialized-value by ltx2018 · Pull Request #476 · libssh2/libssh2 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160967](#) Oracle Enterprise Linux Security Update for libssh2 (ELSA-2023-5615)

[199754](#) Ubuntu Security Notification for libssh2 Vulnerability (USN-6371-1)

[242148](#) Red Hat Update for libssh2 (RHSA-2023:5615)

257258 CentOS Security Update for libssh2
257287 CentOS Security Update for libssh2 (CESA-2023:5615)
296108 Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
356143 Amazon Linux Security Advisory for libssh2 : ALAS2-2023-2257
356158 Amazon Linux Security Advisory for libssh2 : ALAS-2023-1834
356349 Amazon Linux Security Advisory for libssh2 : AL2012-2023-452
379038 Alibaba Cloud Linux Security Update for libssh2 (ALINUX2-SA-2023:0041)
379090 IBM QRadar SIEM Multiple Security Vulnerabilities (7070736)
6000057 Debian Security Update for libssh2 (DLA 3559-1)
754911 SUSE Enterprise Linux Security Update for libssh2_org (SUSE-SU-2023:3738-1)
907343 Common Base Linux Mariner (CBL-Mariner) Security Update for libssh2 (28594-1)

© [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](#)