



CVE-2020-15778

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

Summary

CVE	CVE-2020-15778
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-24 14:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Broadcom	Fabric Operating System	-	All	All	All
Hardware	Netapp	A700s	-	All	All	All
Operating System	Netapp	A700s Firmware	-	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Operating System	Netapp	Brocade Fabric Os	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Hardware	Netapp	Hci Storage Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Openbsd	Openssh	8.3	-	All	All
Application	Openbsd	Openssh	8.3	p1	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Openbsd	Openssh	8.3	-	All	All
Application	Openbsd	Openssh	8.3	p1	All	All

References

Reference	Source	Link	Tags
GitHub - cpandya2909/CVE-2020-15778	MISC	github.com	Exploit, Thir
OpenSSH: Security	MISC	www.openssh.com	Vendor Adv
OpenSSH: Multiple Vulnerabilities (GLSA 202212-06) — Gentoo security	GENTOO	security.gentoo.org	
CVE-2020-15778 OpenSSH Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
Deprecating Scp Hacker News	MISC	news.ycombinator.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [38901](#) OpenSSH Command Injection Vulnerability
- [591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
- [670406](#) EulerOS Security Update for openssh (EulerOS-SA-2021-1993)
- [710695](#) Gentoo Linux OpenSSH Multiple Vulnerabilities (GLSA 202212-06)
- [900081](#) CBL-Mariner Linux Security Update for openssh 8.0p1
- [902817](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (2521)

© [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](#)