



CVE-2018-20685

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

Summary

| | |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2018-20685 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-01-10 21:29:00 UTC |
| Updated | 2023-02-23 23:15:00 UTC |
| Description | In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename |

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|---------------------------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | 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 | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Hardware | Fujitsu | M10-1 | - | All | All | All |
| Operating System | Fujitsu | M10-1 Firmware | All | All | All | All |
| Hardware | Fujitsu | M10-4 | - | All | All | All |
| Hardware | Fujitsu | M10-4s | - | All | All | All |
| Operating System | Fujitsu | M10-4s Firmware | All | All | All | All |

| | | | | | | |
|------------------|---------|-------------------------------------|-----|-----|-----|-----|
| Operating System | Fujitsu | M10-4 Firmware | All | All | All | All |
| Hardware | Fujitsu | M12-1 | - | All | All | All |
| Operating System | Fujitsu | M12-1 Firmware | All | All | All | All |
| Hardware | Fujitsu | M12-2 | - | All | All | All |
| Hardware | Fujitsu | M12-2s | - | All | All | All |
| Operating System | Fujitsu | M12-2s Firmware | All | All | All | All |
| Operating System | Fujitsu | M12-2 Firmware | All | All | All | All |
| Application | Netapp | Cloud Backup | - | All | All | All |
| Application | Netapp | Cloud Backup | - | All | All | All |
| Application | Netapp | Element Software | - | All | All | All |
| Application | Netapp | Element Software | - | All | All | All |
| Application | Netapp | Ontap Select Deploy | - | All | All | All |
| Application | Netapp | Ontap Select Deploy | - | All | All | All |
| Application | Netapp | Steelstore Cloud Integrated Storage | - | All | All | All |
| Application | Netapp | Steelstore Cloud Integrated Storage | - | All | All | All |
| Application | Netapp | Storage Automation Store | - | All | All | All |
| Application | Netapp | Storage Automation Store | - | All | All | All |
| Application | Openbsd | Openssh | All | All | All | All |
| Operating System | Oracle | Solaris | 10 | All | All | All |
| Operating System | Oracle | Solaris | 10 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 8.1 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 8.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 8.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 8.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 8.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 8.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 8.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 8.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 8.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 8.6 | All | All | All |
| Hardware | Siemens | Scalance X204rna | - | All | All | All |
| Hardware | Siemens | Scalance X204rna Eec | - | All | All | All |

| | | | | | | |
|------------------|---------|-------------------------------|-----|-----|-----|-----|
| Operating System | Siemens | Scalance X204rna Eec Firmware | All | All | All | All |
| Operating System | Siemens | Scalance X204rna Firmware | All | All | All | All |
| Application | Winscp | Winscp | All | All | All | All |

References

| Reference | Source | Link |
|------------------------------------------------------------------------------------------------------------------|---------|----------------------------|
| upstream: disallow empty incoming filename or ones that refer to the · openssh/openssh-portable@6010c03 · GitHub | MISC | github.co |
| [SECURITY] [DLA 1728-1] openssh security update | MLIST | lists.debi |
| USN-3885-1: OpenSSH vulnerabilities Ubuntu security notices | UBUNTU | usn.ubun |
| OpenSSH CVE-2018-20685 Access Bypass Vulnerability | BID | www.sec |
| OpenSSH: Multiple vulnerabilities (GLSA 201903-16) — Gentoo security | GENTOO | security.g |
| Debian -- Security Information -- DSA-4387-1 openssh | DEBIAN | www.deb |
| Dropbear: Multiple vulnerabilities (GLSA 202007-53) — Gentoo security | GENTOO | security.g |
| src/usr.bin/ssh/scp.c - diff - 1.198 | MISC | cvsweb.c |
| cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf | CONFIRM | cert-porta |
| Oracle Critical Patch Update - October 2019 | MISC | www.ora |
| Red Hat Customer Portal | REDHAT | access.re |
| CVE-2018-20685 OpenSSH Vulnerability in NetApp Products NetApp Product Security | CONFIRM | security.r |
| sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt | MISC | sintonen. |
| Oracle Critical Patch Update Advisory - April 2019 | MISC | www.ora |
| CVE Program record | CVE.ORG | www.cve |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 296092 Oracle Solaris 11.4 Support Repository Update (SRU) 7.1.4 Missing (CPUJAN2019) |
| 500169 Alpine Linux Security Update for dropbear |
| 500487 Alpine Linux Security Update for openssh |
| 501399 Alpine Linux Security Update for dropbear |
| 503903 Alpine Linux Security Update for dropbear |
| 504246 Alpine Linux Security Update for openssh |
| 591280 Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS) Multiple Vulnerabilities (ICSA-22-349-21, SSA-412672) |

© [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](#)