



CVE-2019-6111

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

Summary

CVE	CVE-2019-6111
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-31 18:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Mina Sshd	2.2.0	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	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
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	12.0	-	All	All
Operating System	Freebsd	Freebsd	12.0	p1	All	All

Operating System	Freebsd	Freebsd	12.0	p2	All	All
Operating System	Freebsd	Freebsd	12.0	p3	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	Openbsd	Openssh	All	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
1677794 – CVE-2019-6111 affects krb5-appl kerberized rcp	MISC	bugzilla.redhat.com
Pony Mail!	MLIST	lists.apache.org
[SECURITY] Fedora 30 Update: openssh-8.0p1-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
[SECURITY] Fedora 30 Update: openssh-8.0p1-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
USN-3885-2: OpenSSH vulnerability Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 1728-1] openssh security update	MLIST	lists.debian.org
oss-security - CVE-2022-29154: Rsync client-side arbitrary file write vulnerability.	MLIST	www.openwall.com
FreeBSD-EN-19:10	FREEBSD	www.freebsd.org
[security-announce] openSUSE-SU-2019:1602-1: moderate: Security update f	SUSE	lists.opensuse.org
USN-3885-1: OpenSSH vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
OpenSSH: Multiple vulnerabilities (GLSA 201903-16) — Gentoo security	GENTOO	security.gentoo.org
Debian -- Security Information -- DSA-4387-1 openssh	DEBIAN	www.debian.org
OpenSSH CVE-2019-6111 Arbitrary File Overwrite Vulnerability	BID	www.securityfocus.com
SCP Client - Multiple Vulnerabilities (SSHtranger Things) - Multiple remote Exploit	EXPLOIT-DB	www.exploit-db.com
cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf	CONFIRM	cert-portal.siemens.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Oracle Critical Patch Update - October 2019	MISC	www.oracle.com
Red Hat Customer Portal	REDHAT	access.redhat.com
January 2019 OpenSSH Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
oss-security - Announce: OpenSSH 8.0 released	MLIST	www.openwall.com
Pony Mail!		lists.apache.org
CVS log for src/usr.bin/ssh/scp.c	MISC	cvsweb.openbsd.org
sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt	MISC	sintonen.fi
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500487 Alpine Linux Security Update for openssh

500107 Alpine Linux Security Update for openssh

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)

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

© [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](#)