



# CVE-2019-6109

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-6109
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-01-31 18:29:00 UTC
<b>Updated</b>	2023-11-07 03:13:00 UTC
<b>Description</b>	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (c

## Risk And Classification

**Problem Types:** CWE-116

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Hardware	<a href="#">Fujitsu</a>	<a href="#">M10-1</a>	-	All	All	All
Operating System	<a href="#">Fujitsu</a>	<a href="#">M10-1 Firmware</a>	All	All	All	All
Hardware	<a href="#">Fujitsu</a>	<a href="#">M10-4</a>	-	All	All	All
Hardware	<a href="#">Fujitsu</a>	<a href="#">M10-4s</a>	-	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	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	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	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
[SECURITY] Fedora 30 Update: openssh-8.0p1-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: openssh-8.0p1-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>

[SECURITY] Fedora 30 Update: openssh-8.0p1-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] [DLA 1728-1] openssh security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[security-announce] openSUSE-SU-2019:1602-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
USN-3885-1: OpenSSH vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
OpenSSH: Multiple vulnerabilities (GLSA 201903-16) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
Debian -- Security Information -- DSA-4387-1 openssh	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf">cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf</a>	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
CVS log for src/usr.bin/ssh/progressmeter.c	MISC	<a href="https://cvsweb.openbsd.org">cvsweb.openbsd.org</a>
Oracle Critical Patch Update - October 2019	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
January 2019 OpenSSH Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
CVS log for src/usr.bin/ssh/scp.c	MISC	<a href="https://cvsweb.openbsd.org">cvsweb.openbsd.org</a>
<a href="https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt">sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt</a>	MISC	<a href="https://sintonen.fi">sintonen.fi</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[376032](#) F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) OpenSSH Vulnerability (K12252011)

[500487](#) 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](#)