



CVE-2019-16905

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

Summary

CVE	CVE-2019-16905
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-09 20:15:00 UTC
Updated	2023-03-01 01:56:00 UTC
Description	OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integ

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Hardware	Siemens	Scalance X204rna	-	All	All	All
Hardware	Siemens	Scalance X204rna Ecc	-	All	All	All
Operating System	Siemens	Scalance X204rna Ecc Firmware	All	All	All	All
Operating System	Siemens	Scalance X204rna Firmware	All	All	All	All

References

Reference

- SSD Advisory - OpenSSH Pre-Auth XMSS Integer Overflow - SSD Secure Disclosure
- Bug 1153537 – VUL-1: CVE-2019-16905: openssh: when compiled with an experimental key type, has a pre-authentication integer overflow if
- src/usr.bin/ssh/sshkey-xmss.c - diff - 1.6
- 0day.life/exploits/0day-1009.html
- oss-security - Announce: OpenSSH 8.1 released

CVS log for src/usr.bin/ssh/sshkey-xmss.c

cert-portal.siemens.com/productcert/pdf/ssa-412672.pdf

OpenSSH: Release Notes

OpenSSH: Integer overflow (GLSA 201911-01) — Gentoo security

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[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)

[710122](#) Gentoo Linux OpenSSH Integer overflow Vulnerability (GLSA 201911-01)

[900092](#) CBL-Mariner Linux Security Update for openssh 8.0p1

[902866](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (2523)

© [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](#)