



# CVE-2020-14145

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

## Summary

<b>CVE</b>	CVE-2020-14145
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-06-29 18:15:00 UTC
<b>Updated</b>	2022-04-28 19:34:00 UTC
<b>Description</b>	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm

## Risk And Classification

**Problem Types:** CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Aff A700s</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Aff A700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Aff A700s Firmware</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Aff A700s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Compute Node</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Compute Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci Management Node</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Storage Node</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Hci Storage Node</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Solidfire</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Steelstore Cloud Integrated Storage</a>	-	All	All	All

Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Openbsd	Openssh	8.4	-	All	All
Application	Openbsd	Openssh	8.5	-	All	All
Application	Openbsd	Openssh	8.6	-	All	All
Application	Openbsd	Openssh	All	All	All	All
Application	Openbsd	Openssh	8.4	-	All	All

## References

Reference	Source	Link	Tags
SSH-MITM Docs - CVE-2020-14145	MISC	<a href="https://docs.ssh-mitm.at">docs.ssh-mitm.at</a>	Third Party Adv
oss-security - Some mitigation for openssh CVE-2020-14145	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing List, Pa
OpenSSH: Multiple vulnerabilities (GLSA 202105-35) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
Detail en : FZI Forschungszentrum Informatik	MISC	<a href="http://www.fzi.de">www.fzi.de</a>	Third Party Adv
ssh-mitm/cve202014145.py at master · ssh-mitm/ssh-mitm · GitHub	MISC	<a href="https://github.com">github.com</a>	Third Party Adv
CVE-2020-14145 OpenSSH Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	Third Party Adv
Comparing V_8_3_P1...V_8_4_P1 · openssh/openssh-portable · GitHub	MISC	<a href="https://github.com">github.com</a>	Patch, Third Pa
openssh.git - Portable OpenSSH	MISC	<a href="https://anongit.mindrot.org">anongit.mindrot.org</a>	Patch, Third Pa
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">159496</a> Oracle Enterprise Linux Security Update for openssh (ELSA-2021-4368)
<a href="#">239822</a> Red Hat Update for openssh (RHSA-2021:4368)
<a href="#">376243</a> F5 BIG-IP Local Traffic Manager (LTM), Application Security Manager (ASM), Access Policy Manager (APM) OpenSSH client Vulnerability (K48050136)
<a href="#">376465</a> F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) OpenSSH Client Vulnerability (K48050136)
<a href="#">38902</a> OpenSSH Man-in-the-Middle (MITM) Attack Vulnerability
<a href="#">500488</a> Alpine Linux Security Update for openssh
<a href="#">501463</a> Alpine Linux Security Update for openssh
<a href="#">504247</a> Alpine Linux Security Update for openssh

<a href="#">591406</a> Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
<a href="#">670195</a> EulerOS Security Update for openssh (EulerOS-SA-2021-1694)
<a href="#">710079</a> Gentoo Linux OpenSSH Multiple vulnerabilities (GLSA 202105-35)
<a href="#">750479</a> OpenSUSE Security Update for openssh (openSUSE-SU-2020:2298-1)
<a href="#">750494</a> OpenSUSE Security Update for openssh (openSUSE-SU-2020:2240-1)
<a href="#">900081</a> CBL-Mariner Linux Security Update for openssh 8.0p1
<a href="#">903500</a> Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (2520)
<a href="#">940145</a> AlmaLinux Security Update for openssh (ALSA-2021:4368)
<a href="#">960784</a> Rocky Linux Security Update for openssh (RLSA-2021:4368)

© [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](#)**