CVE-2020-14145

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-14145
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-29 18:15:00 UTC
Updated	2022-04-28 19:34:00 UTC
Description	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	Netapp	Active Iq Unified Manager	All	All	All	All
Application	Netapp	Active Iq Unified Manager	All	All	All	All
Hardware	Netapp	Aff A700s	-	All	All	All
Hardware	Netapp	Aff A700s	-	All	All	All
Operating System	Netapp	Aff A700s Firmware	-	All	All	All
Operating System	Netapp	Aff A700s Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Hardware	Netapp	Hci Storage Node	-	All	All	All
Hardware	Netapp	Hci Storage Node	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	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	docs.ssh-mitm.at	Third Party Adv
oss-security - Some mitigation for openssh CVE-2020-14145	MLIST	www.openwall.com	Mailing List, Pa
OpenSSH: Multiple vulnerabilities (GLSA 202105-35) — Gentoo security	GENTOO	security.gentoo.org	
Detail en : FZI Forschungszentrum Informatik	MISC	www.fzi.de	Third Party Adv
ssh-mitm/cve202014145.py at master · ssh-mitm/ssh-mitm · GitHub	MISC	github.com	Third Party Adv
CVE-2020-14145 OpenSSH Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	Third Party Adv
Comparing V_8_3_P1...V_8_4_P1 · openssh/openssh-portable · GitHub	MISC	github.com	Patch, Third Pa
openssh.git - Portable OpenSSH	MISC	anongit.mindrot.org	Patch, Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159496 Oracle Enterprise Linux Security Update for openssh (ELSA-2021-4368)

239822 Red Hat Update for openssh (RHSA-2021:4368)

376243 F5 BIG-IP Local Traffic Manager (LTM), Application Security Manager (ASM), Access Policy Manager (APM) OpenSSH client Vulnerability (K48050136)

376465 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) OpenSSH Client Vulnerability (K48050136)

38902 OpenSSH Man-in-the-Middle (MITM) Attack Vulnerability

500488 Alpine Linux Security Update for openssh

501463 Alpine Linux Security Update for openssh

504247 Alpine Linux Security Update for openssh

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

670195 EulerOS Security Update for openssh (EulerOS-SA-2021-1694)

710079 Gentoo Linux OpenSSH Multiple vulnerabilities (GLSA 202105-35)

750479 OpenSUSE Security Update for openssh (openSUSE-SU-2020:2298-1)

750494 OpenSUSE Security Update for openssh (openSUSE-SU-2020:2240-1)

900081 CBL-Mariner Linux Security Update for openssh 8.0p1

903500 Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (2520)

940145 AlmaLinux Security Update for openssh (ALSA-2021:4368)

960784 Rocky Linux Security Update for openssh (RLSA-2021:4368)