CVE-2016-20012

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-20012
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-15 20:15:00 UTC
Updated	2023-11-07 02:30:00 UTC
Description	** DISPUTED ** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of userna

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Openbsd	Openssh	All	All	All	All

References

Reference
openssh-portable/auth2-pubkey.c at d0fffc88c8fe90c1815c6f4097bc8cbcabc0f3dd · openssh/openssh-portable · GitHub
CVE-2016-20012 - Publickey Information leak - Only allow SSH_MSG_USERAUTH_REQUEST with signature by manfred-kaiser · Pull Reque
oss-security - About OpenSSH "user enumeration" / CVE-2018-15473
CVE-2016-20012 OpenSSH Vulnerability in NetApp Products | NetApp Product Security
CVE-2016-20012 - Publickey Information leak - Only allow SSH_MSG_USERAUTH_REQUEST with signature by manfred-kaiser · Pull Reque
Publickey User Enumeration - Only allow SSH_MSG_USERAUTH_REQUEST with signature by manfred-kaiser · Pull Request #270 · openssl
Public SSH keys can leak your private infrastructure | Artem Golubin
Chris's Wiki :: blog/tech/SSHKeysAreInfoLeak
CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

38903 OpenSSH Probable User Enumeration Vulnerability

900458 Common Base Linux Mariner (CBL-Mariner) Security Update for openssh (5921)