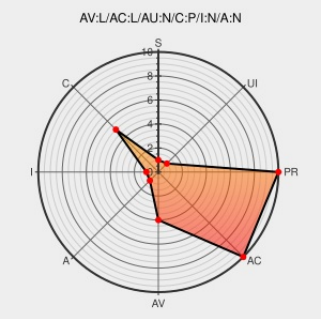
CVE-1999-1010

Published on: 12/14/1999 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:32 PM UTC

CVE-1999-1010

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openssh from Openbsd contain the following vulnerability:

An SSH 1.2.27 server allows a client to use the "none" cipher, even if it is not allowed by the server policy.

CVE-1999-1010 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
'sshd1 allows unencrypted sessions regardless of server policy' - MARC	marc.info text/x-diff	BUGTRAQ 19991214 sshd1 allows unencrypted sessions regardless of server policy

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Openbsd	Openssh	1.2.27	All	All	All
Application	Openbsd	Openssh	1.2.27	All	All	All

cpe:2.3:a:openbsd:openssh:1.2.27:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:1.2.27:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→