CVE-2001-1469

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

Summary

CVE	CVE-2001-1469
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-01-18 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The RC4 stream cipher as used by SSH1 allows remote attackers to modify messages without detection by XORing the ori

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:P/A:N

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ssh	Ssh	1.2.24	All	All	All

Application	Ssh	Ssh	1.2.25	All	All	All
Application	Ssh	Ssh	1.2.26	All	All	All
Application	Ssh	Ssh	1.2.27	All	All	All
Application	Ssh	Ssh	1.2.28	All	All	All
Application	Ssh	Ssh	1.2.29	All	All	All
Application	Ssh	Ssh	1.2.30	All	All	All
Application	Ssh	Ssh	1.2.31	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibmcloud.com	
CERT/CC Vulnerability Note VU#25309	af854a3a-2127-422b-91ae-364da2661108	www.kb.cert.org	Exploit, US Governn
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.