CVE-2001-0259

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

Summary

CVE	CVE-2001-0259
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-06-02 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	ssh-keygen in ssh 1.2.27 - 1.2.30 with Secure-RPC can allow local attackers to recover a SUN-DES-1 magic phrase genera

Risk And Classification

Primary CVSS: v2.0 3.6 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a
Page Not Found. Sorry about that!	af854a3a
Neohapsis Archives - Bugtraq - Bug in SSH1 secure-RPC support can expose users' private keys - From ssh2-bugs@SSH.COM	af854a3a
SSH Secure-RPC Weak Encrypted Authentication Vulnerability	af854a3a
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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