CVE-2011-0539

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

Summary

CVE	CVE-2011-0539
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-10 18:00:57 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The key_certify function in usr.bin/ssh/key.c in OpenSSH 5.6 and 5.7, when generating legacy certificates using the -t comr

Risk And Classification

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

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Openssh	5.6	All	All	All

Application	Openbsd	Openssh	5.7	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
oss-security - Re: [vendor-sec] OpenSSH security advisory: legacy certificate signing in 5.6/5.7	af854a3a-2127-422b-9
OpenSSH Legacy Certificates Stack Memory Leak Weakness - Secunia.com	af854a3a-2127-422b-9
Juniper Networks - 2015-04 Security Bulletin: IDP: Multiple vulnerabilities addressed by third party software updates.	af854a3a-2127-422b-9
OpenSSH Legacy Certificates May Disclose Stack Contents to Remote Users - SecurityTracker	af854a3a-2127-422b-9
OpenSSH Legacy Certificate Signing Information Disclosure Vulnerability	af854a3a-2127-422b-9
IBM X-Force Exchange	af854a3a-2127-422b-9
h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp	af854a3a-2127-422b-9
www.openssh.com/txt/legacy-cert.adv	af854a3a-2127-422b-9
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-9
HP Insight Control for Linux Multiple Vulnerabilities - Secunia.com	af854a3a-2127-422b-9
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.