CVE-2002-0575

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

Summary

CVE	CVE-2002-0575
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-06-18 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in OpenSSH before 2.9.9, and 3.x before 3.2.1, with Kerberos/AFS support and KerberosTgtPassing or AFS

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Openssh	2.1	All	All	All

Application	Openbsd	Openssh	2.1.1	All	All	All
Application	Openbsd	Openssh	2.2	All	All	All
Application	Openbsd	Openssh	2.3	All	All	All
Application	Openbsd	Openssh	2.5	All	All	All
Application	Openbsd	Openssh	2.5.1	All	All	All
Application	Openbsd	Openssh	2.5.2	All	All	All
Application	Openbsd	Openssh	2.9	All	All	All
Application	Openbsd	Openssh	2.9.9	All	All	All
Application	Openbsd	Openssh	2.9p1	All	All	All
Application	Openbsd	Openssh	2.9p2	All	All	All
Application	Openbsd	Openssh	3.0	All	All	All
Application	Openbsd	Openssh	3.0.1	All	All	All
Application	Openbsd	Openssh	3.0.2	All	All	All
Application	Openbsd	Openssh	3.1	All	All	All
Application	Openbsd	Openssh	3.2	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
'OpenSSH 2.2.0 - 3.1.0 server contains a locally exploitable' - MARC	af854a3a-2127-422b-91ae-364c
ISS X-Force Database: openssh-sshd-kerberos-bo (8896): OpenSSH Kerberos 4 TGT/AFS buffer overflow	af854a3a-2127-422b-91ae-364c
SecurityFocus HOME Mailing List: BugTraq	af854a3a-2127-422b-91ae-364c
www.osvdb.org/781	af854a3a-2127-422b-91ae-364c
ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-022.2.txt	af854a3a-2127-422b-91ae-364c
'OpenSSH 3.2.2 released (fwd)' - MARC	af854a3a-2127-422b-91ae-364c
SecurityFocus HOME Mailing List: BugTraq	af854a3a-2127-422b-91ae-364c
Neohapsis Archives - Bugtraq - OpenSSH Security Advisory (adv.token) - From provosciti.umich.edu	af854a3a-2127-422b-91ae-364c
Neohapsis Archives - Bugtraq - TSLSA-2002-0047 - openssh - From tsl@trustix.com	af854a3a-2127-422b-91ae-364c
OpenSSH Kerberos 4 TGT/AFS Token Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364c
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**