CVE-2005-2666

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

Summary

CVE	CVE-2005-2666
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-08-23 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	SSH, as implemented in OpenSSH before 4.0 and possibly other implementations, stores hostnames, IP addresses, and ke

Risk And Classification

Primary CVSS: v2.0 1.2 from nvd@nist.gov

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

Problem Types: CWE-255 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:H/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	3.0	All	All	All

Application	Openbsd	Openssh	3.0.1	All	All	All
Application	Openbsd	Openssh	3.0.1p1	All	All	All
Application	Openbsd	Openssh	3.0.2	All	All	All
Application	Openbsd	Openssh	3.0.2p1	All	All	All
Application	Openbsd	Openssh	3.0p1	All	All	All
Application	Openbsd	Openssh	3.1	All	All	All
Application	Openbsd	Openssh	3.1p1	All	All	All
Application	Openbsd	Openssh	3.2	All	All	All
Application	Openbsd	Openssh	3.2.2p1	All	All	All
Application	Openbsd	Openssh	3.2.3p1	All	All	All
Application	Openbsd	Openssh	3.3	All	All	All
Application	Openbsd	Openssh	3.3p1	All	All	All
Application	Openbsd	Openssh	3.4	All	All	All
Application	Openbsd	Openssh	3.4p1	All	All	All
Application	Openbsd	Openssh	3.5	All	All	All
Application	Openbsd	Openssh	3.5p1	All	All	All
Application	Openbsd	Openssh	3.6	All	All	All
Application	Openbsd	Openssh	3.6.1	All	All	All
Application	Openbsd	Openssh	3.6.1p1	All	All	All
Application	Openbsd	Openssh	3.6.1p2	All	All	All
Application	Openbsd	Openssh	3.7	All	All	All
Application	Openbsd	Openssh	3.7.1	All	All	All
Application	Openbsd	Openssh	3.7.1p2	All	All	All
Application	Openbsd	Openssh	3.8	All	All	All
Application	Openbsd	Openssh	3.8.1	All	All	All
Application	Openbsd	Openssh	3.8.1p1	All	All	All
Application	Openbsd	Openssh	3.9	All	All	All
Application	Openbsd	Openssh	3.9.1	All	All	All
Application	Openbsd	Openssh	3.9.1p1	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
Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org

Repository / Oval Repository	af854a3a-2127-422b-91ae-364da2661108	oval.cisecurity.org
Secunia - Advisories - SCO OpenServer update for OpenSSH	af854a3a-2127-422b-91ae-364da2661108	secunia.com
ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.11/SCOSA-2006.11.txt	af854a3a-2127-422b-91ae-364da2661108	ftp.sco.com
NMS @ MIT CSAIL: Secure Shell Shock	af854a3a-2127-422b-91ae-364da2661108	nms.csail.mit.edu
Page not found | eWEEK	af854a3a-2127-422b-91ae-364da2661108	www.eweek.com
Red Hat Update for Multiple Packages - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Support	af854a3a-2127-422b-91ae-364da2661108	www.redhat.com
Page not found | eWEEK	MITRE	www.eweek.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2006-09-20	Joshua Bressers	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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