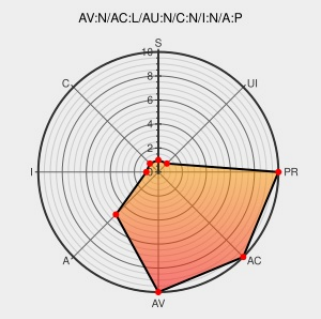
CVE-2006-4925

Published on: 09/28/2006 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:35 AM UTC

CVE-2006-4925

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openssh from Openbsd contain the following vulnerability:

packet.c in ssh in OpenSSH allows remote attackers to cause a denial of service (crash) by sending an invalid protocol sequence with USERAUTH_SUCCESS before NEWKEYS, which causes newkeys[mode] to be NULL.

CVE-2006-4925 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
OpenPKG Corporation: Security: Security Advisories	www.openpkg.org text/html	OPENPKG OpenPKG-SA-2006.022
Gentoo Bug 148228 - net-misc/openssh Multiple minor issues CVE-2006-4924 CVE-2006-4925	Exploit Patch bugs.gentoo.org text/html	MISC bugs.gentoo.org/show_bug.cgi?id=148228
SUSE updates for openssh, openssl, and bind9 - Advisories - Secunia	web.archive.org text/html	SECUNIA 22298
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2006:062
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061005 rPSA-2006-0185-1 gnome-ssh-askpass openssh openssh-client

		openssh-server
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2006:024
SUSE update for openssh - Advisories - Secunia	web.archive.org text/html	SECUNIA 22495
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060927 rPSA-2006-0174-1 gnome-ssh-askpass openssh openssh-client openssh-server
[#RPL-681] multiple vulnerabilities in openssh CVE-2006-4925 CVE-2006-5052 - rPath JIRA	web.archive.org text/html Inactive Link Not Archived	CONFIRM issues.rpath.com/browse/RPL-681
Mandriva update for openssh - Advisories - Secunia	web.archive.org text/html	SECUNIA 22245
IBM HMC OpenSSH / OpenSSL Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 23038
Advisories - Mandriva Linux	www.mandriva.com text/html	MANDRIVA MDKSA-2006:179
[#RPL-661] openssh denial of service CVE-2006-4924 and client unclean exit CVE-2006-4925 - rPath JIRA	web.archive.org text/html Inactive Link Not Archived	CONFIRM issues.rpath.com/browse/RPL-661
src/usr.bin/ssh/packet.c - diff - 1.145	www.openbsd.org text/html	CONFIRM www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/packet.c.diff?r1=1.144&r2=1.145&f=h

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Openssh	4.5	All	All	All
Application	Openbsd	Openssh	4.5	All	All	All

cpe:2.3:a:openbsd:openssh:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.5:*:*:*:*:*:*:*:

← Previous ID

Next ID→

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