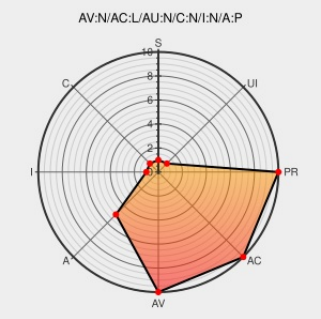
CVE-2004-2069

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2004-2069

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



Certain versions of Openssh from Openbsd contain the following vulnerability:

sshd.c in OpenSSH 3.6.1p2 and 3.7.1p2 and possibly other versions, when using privilege separation, does not properly signal the non-privileged process when a session has been terminated after exceeding the LoginGraceTime setting, which leaves the connection open and allows remote attackers to cause a denial of service (connection consumption).

CVE-2004-2069 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
'OpenSSH - Connection problem when LoginGraceTime exceeds time' - MARC	marc.info text/html	MLIST [openssh-unix-dev] 20040127 OpenSSH - Connection problem when LoginGraceTime exceeds time
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061113 VMSA-2006-0007 - VMware ESX Server 2.1.3 Upgrade Patch 2
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 16567
Secunia - Advisories - SGI Advanced Linux Environment Multiple Updates	web.archive.org text/html	SECUNIA 17135

VMware ESX Server 2.0.2 Upgrade Patch 2 (for 2.0.2 Systems)	www.vmware.com text/html	CONFIRM www.vmware.com/download/esx/esx-202-200610-patch.html
Download Patch ESX-9986131 for VMware ESX Server 3.0.1	www.vmware.com text/html	CONFIRM www.vmware.com/support/vi3/doc/esx-9986131-patch.html
VMWare ESX Server Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 23680
VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 22875
'Re: OpenSSH - Connection problem when LoginGraceTime exceeds time' - MARC	marc.info text/x-diff	MLIST [openssh-unix-dev] 20040128 Re: OpenSSH - Connection problem when LoginGraceTime exceeds time
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11541
VMware ESX Server 2.1.3 Upgrade Patch 2 (for 2.1.3 Systems Only)	www.vmware.com text/html	CONFIRM www.vmware.com/download/esx/esx-213-200610-patch.html
	support.avaya.com application/pdf	CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-216.pdf
Secunia - Advisories - Red Hat update for openssh	web.archive.org text/html	SECUNIA 17000
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061113 VMSA-2006-0008 - VMware ESX Server 2.0.2 Upgrade Patch 2
OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability	cve.report (archive) text/html	BID 14963
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20061113 VMSA-2006-0006 - VMware ESX Server 2.5.3 Upgrade Patch 4
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-4502
	support.avaya.com application/pdf	CONFIRM support.avaya.com/elmodocs2/security/ASA-2005-223.pdf
SecurityFocus	www.securityfocus.com text/html	FEDORA FLSA-2006:168935
rhn.redhat.com | Red Hat Support	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2005:550
Download Patch ESX-3069097 for VMware ESX Server 3.0.1	www.vmware.com text/html	CONFIRM www.vmware.com/support/vi3/doc/esx-3069097-patch.html
Secunia - Advisories - Avaya Intuity LX Two Vulnerabilities	web.archive.org text/html	SECUNIA 17252
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF openssh-sshdc-logingracetime-dos(20930)

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	3.6.1p2	All	All	All
Application	Openbsd	Openssh	3.7.1p2	All	All	All
Application	Openbsd	Openssh	3.6.1p2	All	All	All
Application	Openbsd	Openssh	3.7.1p2	All	All	All

cpe:2.3:a:openbsd:openssh:3.6.1p2:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.7.1p2:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.6.1p2:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:3.7.1p2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→