CVE-2003-0386

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

Summary

CVE	CVE-2003-0386
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-07-02 04:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	OpenSSH 3.6.1 and earlier, when restricting host access by numeric IP addresses and with VerifyReverseMapping disable

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Openssh	3.6.1	All	All	All
Application	Openbsd	Openssh	3.6.1	All	All	All

References

Reference	Source	Link	Tags
Download Patch ESX-9986131 for VMware ESX Server 3.0.1	CONFIRM	www.vmware.com	
VMWare ESX Server Multiple Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com	
ASA-2006-174 (RHSA-2006-0298)	CONFIRM	support.avaya.com	
Apple - Lists.apple.com	CONFIRM	lists.apple.com	
Red Hat update for openssh - Advisories - Secunia	SECUNIA	secunia.com	
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com	
SecurityFocus HOME Mailing List: BugTraq	BUGTRAQ	www.securityfocus.com	Exploit, Patch, Vendor Ac
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia	SECUNIA	secunia.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
20060703-01-P	SGI	patches.sgi.com	
Red Hat update for openssh - Advisories - Secunia	SECUNIA	secunia.com	
CERT/CC Vulnerability Note VU#978316	CERT-VN	www.kb.cert.org	Exploit, Patch, Third Part

rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com	
Download Patch ESX-3069097 for VMware ESX Server 3.0.1	CONFIRM	www.vmware.com	
About Secunia Research | Flexera	SECUNIA	secunia.com	
OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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**