



CVE-2003-0693

Published on: 09/17/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:45 PM UTC

CVE-2003-0693

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openssh](#) from [Openbsd](#) contain the following vulnerability:

A "buffer management error" in `buffer_append_space` of `buffer.c` for OpenSSH before 3.7 may allow remote attackers to execute arbitrary code by causing an incorrect amount of memory to be freed and corrupting the heap, a different vulnerability than CVE-2003-0695.

CVE-2003-0693 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

No Description Provided

[sunsolve.sun.com](#)

[SUNALERT 1000620](#)

Inactive Link Not Archived

[www.openssh.com](#)
[text/x-diff](#)

[CONFIRM www.openssh.com/txt/buffer.adv](#)

[Full-Disclosure] new ssh exploit?

[web.archive.org](#)
[text/html](#)
Inactive Link Not Archived

[FULLDISC 20030915 new ssh exploit?](#)

Mandriva Security Advisories

[www.mandriva.com](#)
[text/html](#)

[MANDRAKE MDKSA-2003:090](#)

redhat.com | Red Hat Support

[www.redhat.com](#)
[text/html](#)

[REDHAT RHSA-2003:280](#)

'[OpenPKG-SA-2003.040] OpenPKG Security Advisory (openssh)' - MARC	marc.info text/html	 BUGTRAQ 20030917 [OpenPKG-SA-2003.040] OpenPKG Security Advisory (openssh)
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:2719
CERT/CC Vulnerability Note VU#333628	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	 CERT-VN VU#333628
Debian -- Security Information -- DSA-383-2 ssh-krb5	www.debian.org Deprecated Link text/html	 DEBIAN DSA-383
'[slackware-security] OpenSSH Security Advisory (SSA:2003-259-01)' - MARC	marc.info text/html	 BUGTRAQ 20030916 [slackware-security] OpenSSH Security Advisory (SSA:2003-259-01)
'OpenSSH Buffer Management Bug Advisory' - MARC	marc.info text/x-diff	 BUGTRAQ 20030916 OpenSSH Buffer Management Bug Advisory
Debian -- Security Information -- DSA-382-3 ssh	www.debian.org Deprecated Link text/html	 DEBIAN DSA-382
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF openssh-packet-bo(13191)
[Full-Disclosure] The lowdown on SSH vulnerability	web.archive.org text/html Inactive Link Not Archived	 FULLDISC 20030916 The lowdown on SSH vulnerability
'TSLSA-2003-0033 - openssh' - MARC	marc.info text/html	 TRUSTIX 2003-0033
'[RHSA-2003:279-01] Updated OpenSSH packages fix potential vulnerability' - MARC	marc.info text/html	 REDHAT RHSA-2003:279
CERT Advisory CA-2003-24 Buffer Management Vulnerability in OpenSSH	US Government Resource www.cert.org text/html	 CERT CA-2003-24
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:447
[Full-Disclosure] openssh remote exploit	web.archive.org text/html Inactive Link Not Archived	 FULLDISC 20030915 openssh remote exploit

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

[illegible]

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023   |

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 registered 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)