



CVE-2005-2797

Published on: 09/06/2005 12:00:00 AM UTC

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

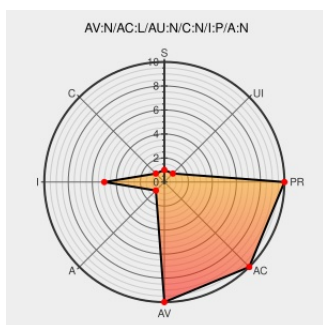
CVE-2005-2797

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

OpenSSH 4.0, and other versions before 4.2, does not properly handle dynamic port forwarding ("-D" option) when a listen address is not provided, which may cause OpenSSH to enable the GatewayPorts functionality.

CVE-2005-2797 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

PARTIAL

NONE

CVE References

Description

Tags

Link

No Description Provided

www.osvdb.org

OSVDB 19142

Inactive Link **Not Archived**

'[OpenPKG-SA-2005.019] OpenPKG Security Advisory (openssh)' - MARC

marc.info
text/html

OPENPKG OpenPKG-SA-2005.019

404 Not Found

[Patch](#)
[Vendor Advisory](#)
www.mindrot.org
[text/html](#)

Inactive Link **Not Archived**

MLIST [openssh-unix-announce] 20050901 Announce: OpenSSH 4.2 released

Secunia - Advisories - Avaya Intuity Audix Two OpenSSH Security Issues

web.archive.org
[text/html](#)

SECUNIA 18661

OpenSSH DynamicForward Inadvertent GatewayPorts Activation

[cve.report \(archive\)](#)

BID 14727

Vulnerability

text/html

ftp.sco.com

text/plain

SCO SCOSA-2005.53

ftp.sco.com

text/plain

SCO SCOSA-2006.11

1. Overview:

support.avaya.com

text/html

SECUNIA 18661

Secunia - Advisories - UnixWare update for openssh

web.archive.org

text/html

SECUNIA 18010

Secunia - Advisories - SCO OpenServer update for OpenSSH

web.archive.org

text/html

SECUNIA 19243

Secunia - Advisories - OpenSSH Two Security Issues

Patch

web.archive.org

text/html

SECUNIA 16686

SecurityTracker: OpenSSH May Unexpectedly Activate GatewayPorts and Also May Disclose GSSAPI Credentials in Certain Cases

securitytracker.com

text/html

SECTrack 1014845

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	4.0	All	All	All
Application	Openbsd	Openssh	4.0	All	All	All

cpe:2.3:a:openbsd:openssh:4.0:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:4.0:*:*:*:*:*:

← Previous ID

Next ID →