

Cisco Security Response: RealVNC Remote Authentication Bypass Vulnerability

Document ID: 70509

<http://www.cisco.com/warp/public/707/cisco-sr-20060622-cmm.shtml>

Revision 1.1

Last Updated 2006 October 11 1900 UTC (GMT)

For Public Release 2006 June 22 1530 UTC (GMT)

Please provide your [feedback](#) on this document.

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

This is Cisco PSIRT's response to the CERT advisory <http://www.kb.cert.org/vuls/id/117929> and acknowledged by Real VNC at <http://www.realvnc.com/products/free/4.1/release-notes.html> . This vulnerability was originally discovered by James Evans.

The original CERT advisory is available at <http://www.kb.cert.org/vuls/id/117929> .

This issue is being tracked by these Cisco bug IDs:

- [CSCse32811](#) ([registered](#) customers only) RealVNC allows remote access to Windows 2000 server console without password.
- [CSCsf02450](#) ([registered](#) customers only) RealVNC allows remote access to IP/VC 3540/DCS server console.

Additional Information

RealVNC is a remote control access product that is bundled with Cisco CallManager and IP/VC 3540/DCS modules to provide remote console access.

A vulnerability in RealVNC may allow a malicious user to bypass RealVNC authentication to gain console access.

In the event that a malicious user exploits this vulnerability to gain console access, all normal CallManager or Windows 2000 security will still apply and is intact. While this vulnerability may provide initial remote access, an attacker will still require Windows and CallManager or IP/VC 3540/DCS credentials to further any attack.

RealVNC has resolved this vulnerability in software version 4.1.2 and later.

Cisco has made available an update for both Call Manager and IP/VC 3540/DCS modules which will update RealVNC to version 4.1.2.

This update for CallManager is available in update win-OS-Upgrade-K9.2000-4-2sr8.exe which may be downloaded at <http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des> ([registered](#) customers only) .

This update for IP/VC 3540/DCS is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/ipvc> ([registered](#) customers only) .

Workaround

The workaround to this issue is to disable the RealVNC service. Please consult RealVNC documentation for further details at <http://www.realvnc.com/documentation.html> .

Revision History

Revision 1.1	2006-October-11	Added information on IPVC 3540/DCS.
Revision 1.0	2006-June-22	Initial public release.

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 11, 2006

Document ID: 70509
