Cisco Security Advisory

Voice Product Vulnerabilities on IBM Servers

Advisory ID: cisco-sa-20040121-voice
Published: 2004 January 21 17:00 GMT
Version1.0: Final
Workarounds: See below

Download CVRF
Download PDF
Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Summary

The default installation of Cisco voice products on the IBM platform will install the Director Agent in an unsecure state, leaving the Director services vulnerable to remote administration control and/or Denial of Service attacks. The vulnerabilities can be mitigated by configuration changes and Cisco is providing a repair script that will close the vulnerable ports and put the Director agent in secure state without requiring an upgrade.

This advisory will be available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040121-voice.

Affected Products

Vulnerable Products

Cisco voice products running on IBM servers installed with the default configurations are affected if they leave TCP or UDP port 14247 open. To verify this vulnerability, the administrator may open a command window on the server and type **netstat -a**. If port 14247 is listed, the server is vulnerable to remote administrative control and Denial of Service attacks.

Affected Cisco voice products:

- Cisco CallManager
- Cisco IP Interactive Voice Response (IP IVR)
- Cisco IP Call Center Express (IPCC Express)
- Cisco Personal Assistant (PA)
- Cisco Emergency Responder (CER)
- Cisco Conference Connection (CCC)
- Cisco Internet Service Node (ISN) running on an IBM with an affected OS version.

Affected IBM-based server model numbers:

- IBM X330 (8654 or 8674)
- IBM X340
- IBM X342
- IBM X345
- MCS-7815-1000
- MCS-7815I-2.0
- MCS-7835I-2.4
- MCS-7835I-3.0

Affected OS Versions:

All operating system (OS) versions running on an IBM server prior to OS 2000.2.6, which has not yet been released as of the date of this notice.

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

The default installations of Cisco voice products on IBM servers will install IBM Director in unsecure state leaving TCP and UDP ports 14247 open. Any Director Server/Console agent can connect over port 14247 to gain administrative level control without requiring authentication. Also, a network security scanner scanning port 14247 can trigger the IBM Director agent process twgipc.exe to use 100% of the CPU until the server is rebooted. These vulnerabilities are documented in the two Cisco bug IDs:

- **CSCed33037 - IBM Director agents default install allows remote access.**
- **CSCed23357 - IBM servers with Director agent 2.2 or 3.11 are vulnerable to a DoS.**

Workarounds

Cisco's repair script adds 3 levels of improved security to the Director agent:

1. The Director agent no longer listens on TCP or UDP ports 14247 for remote connections from a Director Server. This change prevents the Denial of Service attacks described in the Impact section.
2. The repair script secures the Director agent such that even if port 14247 is reenabled, the Director agent still would not accept connections from any Director Server.
3. The Director Agent executable files which are not necessary to the functioning of the program, yet provide high levels of access or control, are completely disabled by this repair script.

Note: If you are using IBM Director Server and Console to monitor the Cisco voice products, this repair script will disable the connection to those IBM servers. The Director agents will still provide pop-up warnings and Event Viewer messages in version 3.11, and SNMP traps to network management software like CiscoWorks IP Telephony Monitor. To regain IBM Director Server monitoring capabilities, IBM Director agent 4.11 will be released in OS Upgrade 2000.2.6 and support can be re-enabled for Director Server after the upgrade to OS version 2000.2.6.

Fixed Software

When considering software upgrades, also consult http://www.cisco.com/go/psirt and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

The vulnerabilities are specific to Cisco voice products on IBM servers and all vulnerabilities listed in this advisory can be mitigated with the repair script without requiring an upgrade.

The repair script is available at:
http://www.cisco.com/pcgi-bin/tablebuild.pl/cmva-3des

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040121-voice

---

Revision History

Revision 1.0	2004-January-21	Initial public release.
