

# [NEWS] Cisco Voice Products Vulnerabilities on IBM Servers

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0068.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 01/22/04

To: list@securiteam.com

Date: 22 Jan 2004 15:03:01 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Cisco Voice Products Vulnerabilities on IBM Servers

---

## 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.

## DETAILS

### Vulnerable Systems:

- \* 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)

## Securiteam: [NEWS] Cisco Voice Products Vulnerabilities on IBM Servers

- \* IBM X340
- \* IBM X342
- \* IBM X345
- \* MCS-7815-1000
- \* MCS-7815I-2.0
- \* MCS-7835I-2.4
- \* MCS-7835I-3.0

\* 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.

The default installation of Cisco voice products on IBM servers will install IBM Director in an insecure 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.

Administrative level control includes the following functionality: shutdown/power off/restart, remote command shell, file transfer, processes/services/device drivers stop and start, network configuration modification (including domain/workgroup membership), Windows 2000 user account creation, and SNMP configuration modification.

In a Denial of Service attack, an attacker can render the Cisco voiceserver inoperative with CPU utilization spiking to 100%, and the IBMserver must be powered off or rebooted in order to regain control of the machine.

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.

Detecting the vulnerability:

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.

Workarounds:

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

- \* 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 above.
- \* 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.
- \* The Director Agent executable files which are not necessary to the functioning of the program, yet provide high levels of access or control,

## Securiteam: [NEWS] Cisco Voice Products Vulnerabilities on IBM Servers

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 Cisco Works 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.

### Solution:

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.

The script can be obtained from:

<<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>>  
<http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des>

As the mitigation for the vulnerabilities is a repair script, a software upgrade is not required to address the vulnerabilities. However, if you have a service contract, and wish to upgrade to unaffected code, you may obtain upgraded software through your regular update channels once that software is available. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Website at <<http://www.cisco.com>> <http://www.cisco.com>.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@cisco.com>> Cisco Systems Product Security Incident Response Team

The official advisory can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20040121-voice.shtml>>  
<http://www.cisco.com/warp/public/707/cisco-sa-20040121-voice.shtml>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.