

**Press Contacts:**

Perveen Akhtar  
Cisco Systems  
+44 (0) 020 8824 4478  
pakhtar@cisco.com

Debbie Leah  
Insight Marketing & Communications  
+44 (0) 1625 500800  
[dleah@insightmkt.com](mailto:dleah@insightmkt.com)

## Cisco Earns Top Rating in Challenging VoIP Security Test

LONDON, UK, May 26, 2004 - Cisco Systems® today announced that its Internet Protocol (IP) telephony system has earned Miercom's highest security rating after sustaining three days of grueling, round-the-clock tests conducted by sophisticated "hackers" looking for security vulnerabilities.

"Cisco proved it can build a Voice over IP (VoIP

<javascript:openGlossary('http://business.cisco.com/app/search.taf?\_function=search&style=iQ&asset\_type\_id=44728&display\_option=Glossary&public\_view=true&kbns=1&keyword=VoIP')>) network that sophisticated hackers were not able to break or even noticeably disturb," said Ed Mier, president of Miercom, a leading network consultancy and product test centre.

"Cisco's 'secure' rating on the Miercom VoIP-Security Rating Scale was the highest of all the vendors who participated," Mier added. "Cisco has set the bar that other IP telephony <javascript:openInfoPage('http://newsroom.cisco.com/dlls/innovators/VoIP/index.html')> vendors will now try to reach. Overall, the IP telephony industry should derive great comfort from these test results."

Miercom tested the Cisco CallManager-based system, the core of its IP Communications system, as well as two entries from Avaya. The full results of the security test have been published in Network World Magazine at:

<<http://www.nwfusion.com/reviews/2004/0524voipsecurity.html?page=1>>

### About the Test

The objective of the attacks was to disrupt IP phone communications. Via each of the assault points, the hackers used scanning tools and techniques to discover what they could about the topology and then launched numerous sophisticated Denial of Service attacks. The attacks attempted to disable devices and functions at all network layers.

After three full days of testing on the Cisco CallManager

<javascript:openInfoPage('http://www.cisco.com/en/US/products/sw/voicesw/ps556/index.html')> system, no perceptible disruption was achieved, according to Miercom. All the capabilities and features that Cisco employed in its test system are currently available to customers.

The hacker team consisted of coordinated local and remote assailants who delivered a "moderate intensity" assault. A set of ground rules limited the hackers to using only

existing tools available on the Web and restricted their access to several specific assault points. The hackers operated with no prior knowledge of the internal network or configuration.

For Cisco, this accomplishment marks another major milestone for its IP Communications business. "Winning this security test on the heels of two recent victories in competitive public reviews clearly position Cisco as having the best overall IP PBX <javascript:openGlossary('http://business.cisco.com/app/search.taf?\_function=search&style=iQ&asset\_type\_id=44728&display\_option=Glossary&public\_view=true&kbns=1&keyword=PBX')> system in the world," said Don Proctor, vice president and general manager of the Cisco Voice Technology Group. "This security evaluation was grueling and featured a sophisticated series of tests designed to uncover security vulnerabilities. The results speak for themselves. They validate that as the network's strategic importance increases and the need to protect critical business applications is amplified, the Cisco Self-Defending Network <javascript:openInfoPage('http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking\_solutions\_package.html')> strategy of identifying, defending and adapting to security threats is a highly reliable way to protect your IT infrastructure and critical business applications."

#### Keys to Success

Miercom tested the Cisco CallManager 4.0 system, which contains a number of new security enhancements. The IP based call processing engine extends the capabilities of the Cisco intelligent self-defending network to better protect Cisco IP Communications <javascript:openInfoPage('http://www.cisco.com/offer/tdm\_home/iptelephony/')> systems and provide improved business resilience. New industry-standard digital certificates in Cisco CallManager 4.0 confirm the identity of network devices to help protect against entry of rogue system users. New standards-based authentication and encryption have been added to Cisco CallManager 4.0 and Cisco IP phones providing end-to-end privacy and integrity of voice communications.

Business resilience has also been enhanced with the new Cisco Security Agent <javascript:openInfoPage('http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html')> (CSA), which is a key component of Cisco's overall security strategy. CSA provides proactive and adaptive threat protection for Cisco telephony applications, servers and desktop computing systems. It brings together multiple levels of security functionality by combining host intrusion prevention, distributed firewall <javascript:openInfoPage('http://business.cisco.com/app/search.taf?\_function=search&style=iQ&asset\_type\_id=44728&display\_option=Glossary&public\_view=true&kbns=1&keyword=firewall')>, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package. Cisco CallManager 4.0 customers, as well as Cisco Unity and Cisco IP Contact Center customers, receive all of these additional levels of safety and protection for their converged networks at no extra cost.

That Cisco IP Communications system tested by Miercom was built around a resilient Cisco data network infrastructure configured according to the Cisco SAFE blueprints for secure communications. This included a strong compliment of layer 2 security features such as DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Port Security and VLAN

<javascript:openGlossary('http://business.cisco.com/app/search.taf?\_function=search&style=iQ&asset\_type\_id=44728&display\_option=Glossary&public\_view=true&kbns=1&keyword=VLAN')> ACLs; stateful firewalls with application inspection capabilities; policers to limit DoS and distributed DoS attacks; and out-of-band management.

#### About Cisco IP Communications

Cisco IP Communications is a comprehensive system of enterprise-class solutions including IP telephony, unified communications, rich media IP audio and videoconferencing, IP video broadcasting and customer contact solutions that take advantage of customers' existing Cisco IP infrastructure to deliver new converged applications. A video interview with the principals at Miercom is available at: <[http://cisco.feedroom.com/index.jsp?fr\\_story=c339e48a0bf94e901fbeaa268d46c2fe2949da8b](http://cisco.feedroom.com/index.jsp?fr_story=c339e48a0bf94e901fbeaa268d46c2fe2949da8b)>. More information about Cisco IP Communications is available at: <<http://newsroom.cisco.com/dlls/innovators/VoIP/index.html>>. More information on Cisco's Self-Defending Network security strategy is available at: <<http://www.cisco.com/go/selfdefend/>>

#### About Miercom

Miercom, founded in 1988, is an independent networking consultancy and product-test center located in Cranbury, NJ. Miercom developed the industry's first comparative test methodologies for testing VoIP equipment. Miercom is a member of the Network World Global Test Alliance and the test lab of record for Business Communications Review (BCR). For more information about Miercom and their new "2004: A VoIP Security Assessment" special report, please visit: <<http://www.miercom.com/>>.

#### About Cisco Systems

Cisco Systems (NASDAQ: CSCO) is the worldwide leader in networking for the Internet. Cisco news and information are available at <<http://www.cisco.com/>>.

###

Copyright© 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and Cisco Unity are registered trademarks or trademarks of Cisco Systems, Inc. and its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners.