

Table of Contents

| | |
|---|---|
| <u>Cisco Security Advisory: Default SNMP Community Strings in Cisco IP/VC Products</u> | 1 |
| <u>Document ID: 63894</u> | 1 |
| <u>Revision 1.0</u> | 1 |
| <u>For Public Release 2005 February 02 16:00 UTC (GMT)</u> | 1 |
| <u>Please provide your feedback on this document</u> | 1 |
| <u>Summary</u> | 1 |
| <u>Affected Products</u> | 1 |
| <u>Vulnerable Products</u> | 1 |
| <u>Products Confirmed Not Vulnerable</u> | 2 |
| <u>Details</u> | 2 |
| <u>Impact</u> | 2 |
| <u>Software Versions and Fixes</u> | 2 |
| <u>Obtaining Fixed Software</u> | 2 |
| <u>Workarounds</u> | 3 |
| <u>Exploitation and Public Announcements</u> | 3 |
| <u>Status of This Notice: FINAL</u> | 3 |
| <u>Distribution</u> | 3 |
| <u>Revision History</u> | 4 |
| <u>Cisco Security Procedures</u> | 4 |

Cisco Security Advisory: Default SNMP Community Strings in Cisco IP/VC Products

Document ID: 63894

Revision 1.0

For Public Release 2005 February 02 16:00 UTC (GMT)

Please provide your feedback on this document.

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Obtaining Fixed Software
Workarounds
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Summary

Hard-coded Simple Network Management Protocol (SNMP) community strings are present in Cisco IP/VC Videoconferencing System models 3510, 3520, 3525 and 3530. Any user who has access to the vulnerable devices and knows the community strings, can obtain total control of the device.

Cisco strongly recommends that all users deploy the mitigation measures outlined in the Workaround section.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050202-ipvc.shtml>.

Affected Products

Vulnerable Products

The following products are known to be vulnerable:

- Cisco IPVC-3510-MCU
- Cisco IPVC-3520-GW-2B
- Cisco IPVC-3520-GW-4B
- Cisco IPVC-3520-GW-2V
- Cisco IPVC-3520-GW-4V
- Cisco IPVC-3520-GW-2B2V
- Cisco IPVC-3525-GW-1P

- Cisco IPVC-3530-VTA

Products Confirmed Not Vulnerable

The following products are known not to be vulnerable:

- Cisco IPVC-3511-MCU
- Cisco IPVC-3511-MCU-E
- Cisco IPVC-3521-GW-4B
- Cisco IPVC-3526-GW-1P
- Cisco IPVC-3540-EMP
- Cisco IPVC-3540-EMP3
- Cisco IPVC-3540-MCU03A
- Cisco IPVC-3540-MCU06A
- Cisco IPVC-3540-MCU10A
- Cisco IPVC-3540-GW2P
- Cisco IPVC-3540-GW4S

No other Cisco products are currently known to be affected by this vulnerability. In particular, video-enabled Cisco IP video telephones are not affected.

Details

Affected products contain hard-coded SNMP community strings. SNMP is used for managing and monitoring an IP/VC device and community strings are the equivalent to a password. All models listed as affected are vulnerable regardless of the software release they are running.

There is no Cisco bug ID associated with this issue.

Impact

A user with knowledge of the community strings can gain full control of the device. Such user can, among other things, create new services, terminate or affect existing sessions, and redirect traffic to a different destination.

Software Versions and Fixes

Cisco will not provide fixed software for this vulnerability. Customers are strongly advised to deploy the mitigation measures described in the Workaround section.

Obtaining Fixed Software

There is no fixed software for this issue. All customers are strongly advised to deploy the mitigation measures. Additionally, customers who are considering replacing the affected models can contact their Cisco sales representative.

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco Technical Assistance Center (TAC).

- +1 800 553 2447 (toll free from within North America)

- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

See <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Workarounds

The only mitigation for this vulnerability is to disable SNMP traffic at the switch port that is connected to the affected device. If that cannot be done, the SNMP traffic to the IP/VC device should be blocked at the nearest possible point. In order for the mitigation to be successful all possible paths to the device must be protected. This can be done by blocking traffic on UDP (User Datagram Protocol) ports 161 and 162. Port 161 is used for inbound/outbound read/write SNMP access and port 162 is used for outbound traffic for SNMP traps. Blocking these ports disables all configuration and traps to/from the device. Access to ports 161 and 162 from the trusted hosts should be temporarily enabled and the IPVC Configuration Utility used when configuration changes are required on the affected IP/VC device.

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

Exploitation and Public Announcements

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

Status of This Notice: FINAL

THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE ADVISORY OR MATERIALS LINKED FROM THE ADVISORY IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS NOTICE AT ANY TIME.

A stand-alone copy or paraphrase of the text of this security advisory that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20050202-ipvc.shtml>.

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP

key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- vulnwatch@wulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.netsys.com
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

| | | |
|--------------|------------------|------------------------|
| Revision 1.0 | 2005-February-02 | 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>.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Feb 02, 2005

Document ID: 63894
