

Table of Contents

<u>Cisco Security Advisory: Fixed SNMP Communities and Open UDP Port in Cisco 7920 Wireless IP Phone</u>	1
<u>Document ID: 68179</u>	1
<u>Advisory ID: cisco-sa-20051116-7920</u>	1
<u>http://www.cisco.com/warp/public/707/cisco-sa-20051116-7920.shtml</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2005 November 16 1600 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	2
<u>Vulnerable Products</u>	2
<u>Products Confirmed Not Vulnerable</u>	2
<u>Details</u>	2
<u>Impact</u>	2
<u>Software Versions and Fixes</u>	2
<u>Workarounds</u>	3
<u>Obtaining Fixed Software</u>	3
<u>Customers with Service Contracts</u>	4
<u>Customers using Third-party Support Organizations</u>	4
<u>Customers without Service Contracts</u>	4
<u>Exploitation and Public Announcements</u>	4
<u>Status of This Notice: FINAL</u>	4
<u>Distribution</u>	5
<u>Revision History</u>	5
<u>Cisco Security Procedures</u>	5

Cisco Security Advisory: Fixed SNMP Communities and Open UDP Port in Cisco 7920 Wireless IP Phone

Document ID: 68179

Advisory ID: cisco-sa-20051116-7920

<http://www.cisco.com/warp/public/707/cisco-sa-20051116-7920.shtml>

Revision 1.0

For Public Release 2005 November 16 1600 UTC (GMT)

Please provide your feedback on this document.

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

Summary

The Cisco 7920 Wireless IP Phone provides Voice Over IP service via IEEE 802.11b Wi-Fi networks and has a form-factor similar to a cordless phone. This product contains two vulnerabilities:

The first vulnerability is an SNMP service with fixed community strings that allow remote users to read, write, and erase the configuration of an affected device.

The second vulnerability is an open VxWorks Remote Debugger on UDP port 17185 that may allow an unauthenticated remote user to access debugging information or cause a denial of service.

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051116-7920.shtml>.

Affected Products

Vulnerable Products

- Cisco 7920 Wireless IP Phone, firmware version 2.0 and earlier

Products Confirmed Not Vulnerable

- Cisco 7920 Wireless IP Phone, firmware version 2.01

No other Cisco products are currently known to be affected by these vulnerabilities, including other IP telephony products.

Details

Fixed SNMP Community Strings

The Cisco 7920 Wireless IP Phone provides an SNMP service with fixed read-only and read-write community strings of "public" and "private", respectively. These strings cannot be changed by the user and will allow remote users to issue an SNMP GetRequest or SetRequest to the phone. SNMP can be used to retrieve and modify the device configuration, including stored user data such as phone book entries. To address this vulnerability, Cisco has provided updated software that removes the SNMP functionality from this product.

This issue is documented in Cisco bug ID CSCsb75186 (registered customers only) .

VxWorks Debugger Port (wdbrpc, 17185/udp)

The Cisco 7920 Wireless IP Phone listens on UDP port 17185 to allow connections from a VxWorks debugger. This port may allow remote users to collect debugging information or conduct a denial of service attack against an affected device. To address this vulnerability, Cisco has provided updated software that closes UDP port 17185.

This issue is documented in Cisco bug ID CSCsb38210 (registered customers only) .

Impact

Successful exploitation of these vulnerabilities may result in information leakage or denial of service attacks against an affected device. In the case of the Fixed SNMP Community Strings vulnerability, an attack may take the form of erasure or modification of the device configuration and personal user data.

Software Versions and Fixes

Cisco has provided free software to address these vulnerabilities; please consult the chart below for details.

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

Cisco Security Advisory: Fixed SNMP Communities and Open UDP Port in Cisco 7920 Wireless IP Phone

new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Cisco Bug ID	Affected Firmware Releases	First Fixed Firmware Release
CSCsb75186 (registered customers only) (SNMP)	Release 1.0(8) and earlier	Release 1.0(9)
CSCsb38210 (registered customers only) (VxWorks)	Release 2.0 and earlier	Release 2.01

Workarounds

- For sites that restrict Cisco 7920 phones to one or more known subnets, Access Control Lists (ACLs) can be used to deny traffic to the affected ports.

The following extended access-list can be adapted to your network. This example assumes that all Cisco 7920 phones are connected to the 192.168.10.0 network and that all SNMP access is to be restricted to a management station with the IP address of 10.1.1.1:

```
access-list 101 permit udp host 10.1.1.1 192.168.10.0 0.0.0.255 range 161 162
access-list 101 permit udp host 10.1.1.1 192.168.10.0 0.0.0.255 port 17185
access-list 101 deny udp any 192.168.10.0 0.0.0.255 range 161 162
access-list 101 deny udp any 192.168.10.0 0.0.0.255 port 17185
access-list 101 permit ip any any
```

The access-list must then be applied to all interfaces using configuration commands such as:

```
interface ethernet 0/0
ip access-group 101 in
```

- Infrastructure ACLs (iACL)

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for iACLs:

<http://www.cisco.com/warp/public/707/iacl.html>

Obtaining Fixed Software

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

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>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix 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 or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +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

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <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.

Exploitation and Public Announcements

This vulnerability was reported to Cisco by Shawn Merdinger and will be disclosed on November 16, 2005 at the CSI 32nd Annual Computer Security conference in Washington, DC. The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this advisory.

Status of This Notice: FINAL

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

A stand-alone copy or Paraphrase of the text of this document 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-20051116-7920.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
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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-November-16	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/en/US/products/products_security_vulnerability_policy.html. 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: Nov 16, 2005

Document ID: 68179
