

Table of Contents

<u>Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access</u>	1
<u>Document ID: 65152</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2005 June 08 2000 UTC (GMT)</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Details</u>	1
<u>Workarounds and Mitigations</u>	2
<u>Acknowledgment</u>	2
<u>Status of This Notice: FINAL</u>	2
<u>Revision History</u>	2
<u>Cisco Security Procedures</u>	2
<u>Related Information</u>	3

Cisco Security Notice: Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access

Document ID: 65152

Revision 1.0

For Public Release 2005 June 08 2000 UTC (GMT)

Please provide your feedback on this document.

Summary
Details
Workarounds and Mitigations
Acknowledgment
Status of This Notice: FINAL
Revision History
Cisco Security Procedures
Related Information

Summary

This Cisco Security Notice is being released in response to the Cisco 802.1x Voice-Enabled Interfaces Allow Anonymous Voice VLAN Access advisory published on June 8, 2005 by FishNet Security at <http://www.fishnetsecurity.com/csirt/disclosure/cisco/>.

This notice will be posted at <http://www.cisco.com/warp/public/707/cisco-sn-20050608-8021x.shtml>

Details

The advisory from FishNet asserts "Voice VLAN access abuse is possible by spoofing Cisco Discovery Protocol (CDP) on voice-enabled Cisco switch interfaces even if 802.1x port-level security is enabled".

Cisco acknowledges that Cisco IP Phones do not currently contain 802.1x supplicants, and are authorized to join the voice VLAN without 802.1x authentication.

Cisco does provide the means for a host attached to the IP Phone enabled-switch port on the back of the phone to run an 802.1x supplicant and the host can only gain access to the data VLAN after either the user, the machine, or both have been properly authenticated via 802.1x.

CDP itself should not be regarded as a security mechanism. CDP is merely an auto-discovery protocol allowing Cisco devices to dynamically learn of any directly attached Cisco devices. In the case of a Cisco IP Phone, CDP is used to obtain node identifying information and in turn inform the node of the proper VLAN assignment.

As the 802.1x standard is written today, it allows for either a single MAC address or multiple MAC addresses to be authenticated on a switch port. There currently is no provision in the standard for authentication of devices per VLAN on a single port. 802.1x authentication is a valuable mechanism to ensure authorized admittance into a network, but should be used in conjunction with a number of other security features to provide the best practice defense-in-depth security in order to control activities and ensure network integrity.

Workarounds and Mitigations

Customers running newer versions of software on their Cisco Catalyst switches can take advantage of a number of features which can aid in limiting what a device can do while on the network. These features include, but are not limited to, DHCP Snooping and Port Security, Dynamic ARP Inspection (DAI) and IP Source Guard.

The whitepaper entitled Cisco Catalyst Integrated Security—Enabling the Self-Defending Network introduces the features on the Catalyst switches which can mitigate Layer 2 and Layer 3 attacks against the switch and devices connected through it.

Additionally, customers running newer versions of Cisco CallManager can take advantage of features now offered on the Cisco IP Phones and CallManager to address Layer 2 and Layer 3 based network attacks, including certificate based authentication and encryption of voice signaling and media to protect the identity, integrity, and privacy of all voice communications.

The product data sheet for Cisco CallManager Version 4.1 lists the features available for further protection of the CallManager and IP Phones.

Acknowledgment

Cisco would like to thank FishNet Security for their cooperation on this issue.

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.

Revision History

Revision 1.0	2005-June-8	Initial 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>.

Related Information

- **Fishnet Advisory**
 - **Cisco Catalyst Integrated Security—Enabling the Self-Defending Network**
 - **Cisco CallManager Version 4.1**
-

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

Updated: Aug 02, 2005

Document ID: 65152
