Cisco Security Notice: Crafted DNS Packet Can Cause Denial Of Service

Revision 1.1

For Public Release 2005 May 24 1200 UTC (GMT)

Please provide your feedback on this document.

Contents

Summary

Some Domain Name System (DNS) implementations may be vulnerable to a Denial of Service attack after receiving and processing a specially crafted DNS packet.

Cisco has made free software available to address this vulnerability.

This security notice is posted at http://www.cisco.com/warp/public/707/cisco-sn-20050524-dns.shtml.

Details

Hosts connected to an IP network use the DNS protocol to resolve names to IP addresses. The protocol is documented in multiple IETF (Internet Engineering Task Force) RFCs (Request For Comments). RFC-1035 defines the protocol specification and options, including a Message compression scheme (section 4.1.4). An attacker can craft a DNS packet containing invalid information in the compressed

section, which can result in an error in processing on the receiving host.

This issue is documented in the following bug IDs:

- **CSCsa67687** (registered customers only) -- IP Phones 7902/7905/7912
- **CSCsa67666** (registered customers only) -- ATA 186/188
- **CSCeh63819** (registered customers only) -- Unity Express
- **CSCeh59380** (registered customers only) -- ACNS devices
- **CSCei01975** (registered customers only) -- Cisco Subscriber Edge Services Manager (SESM)

Symptoms

Successful exploitation of this vulnerability could cause the affected device to crash or to function abnormally, which would generate a Denial of Service condition.

Affected Products

The following products are affected by this vulnerability:

- Cisco IP Phones 7902/7905/7912
- Cisco ATA (Analog Telephone Adaptor) 186/188
- Cisco Unity Express
- Cisco ACNS (Application and Content Networking System) devices, including:
  - Cisco 500 Series Content Engines
  - Cisco 7300 Series Content Engines
  - Cisco Content Routers 4400 series
  - Cisco Content Distribution Manager 4600 series
  - Cisco Content Engine Module for Cisco 2600, 2800, 3600, 3700, and 3800 series Integrated Service Routers
- Cisco SESM (Cisco Subscriber Edge Services Manager)

Unaffected Products

The following products are not vulnerable:

- Any Cisco device running Cisco IOS®
- Any Cisco device running Cisco CatOS
- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco BBSM (Building Broadband Service Manager)
- Cisco Content Switching Module (CSM) for Cisco Catalyst 6500 Series
- Cisco CRS-1
- Cisco CSS-11000 series (Content Services Switches)
- Cisco DistributedDirector
- Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series and Cisco 7600 Series
- Cisco GSS (Global Site Selector) 4490
- Cisco IP Conference Station 7936
- Cisco IP Phones 7920/7940G/7960G/7970
- Cisco LocalDirector
- Cisco Network Registrar (CNR)
- Cisco PIX Security Appliances
- Cisco Secure IDS Appliances and service modules (including IDSM-2)

- Cisco URT/VPS (User Registration Tool/VLAN Policy Server)

No other Cisco products are currently known to be affected by this vulnerability.

Software Versions and Fixes

When considering software upgrades, please also consult http://www.cisco.com/en/US/products/products_security_advisories_listing.html 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 new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") for assistance.

Each row of the products table below lists the earliest possible release that contains the fix (**First Fixed Release**) and the anticipated date of availability. A product running a release that is earlier than the listed release (less than the **First Fixed Release**) is known to be vulnerable. The product should be upgraded at least to the indicated release or a later release (greater than or equal to the **First Fixed Release** label).

Product	Affected Version	First Fixed Release
Cisco SESM	Versions 3.2(1), 3.2(2) and 3.3(1)	Upgrade to 3.3(2), available now on CCO
Cisco IP Phones 7902/7905/7912	SCCP: all versions up to but not including v6.1.1 SIP: all versions up to but not including v1.3.1 H323: all versions up to but not including v1.0.2	SCCP: v6.1.1 - available end of May, 2005 SIP: v1.3.1 - available end of June, 2005 H323: v1.0.2 - availability TBD
ATA 186/188	SCCP: all versions up to but not including v3.2.1 SIP: all versions up to but not including v3.2.1 H323: all versions up to but not including v3.1.3	SCCP: v3.2.1 - available end of May, 2005 SIP: v3.2.1 - available end of June, 2005 H323: v3.1.3 - availability TBD

	MGCP: all versions up to but not including v3.1.2	MGCP: v3.1.2 - availability TBD
Unity Express	all versions up to but not including 2.1.3	2.1.3 - available end of July, 2005.
ACNS devices	all 4.x releases	upgrade to 5.1.15, 5.2.7 or 5.3.3
ACNS devices	all 5.0 releases	upgrade to 5.1.15, 5.2.7 or 5.3.3
ACNS devices	all 5.1 releases up to but not including 5.1.15	upgrade to 5.1.15
ACNS devices	all 5.2 releases up to but not including 5.2.7	upgrade to 5.2.7 - available end of July 2005
ACNS devices	all 5.3 releases up to but not including 5.3.3	upgrade to 5.3.3 - available end of June 2005

Obtaining Fixed Software

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 assistance with the upgrade, which should be free of charge.

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

Please 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.

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

As the fix for this vulnerability is a default configuration change, and a workaround is available, a software upgrade is not required to address this vulnerability. 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 Web site at http://www.cisco.com.

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 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.

There are no workarounds identified for this vulnerability. However, these attacks can be mitigated by securing the Layer-2 infrastructure to reduce exposure on locally controlled networks. Refer to SAFE Layer 2 Security In-depth Version 2 for information on how to secure your L2 (Layer-2) infrastructure. It is important to note that implementing those recommendations will only help against Man-In-The-Middle (MITM) type of attacks in locally controlled networks and not against attacks being performed in networks out of the organization control.

Status of This Notice: FINAL

This is a final notice. Although Cisco cannot guarantee the accuracy of all statements in this notice, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this notice unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this notice.

A stand-alone copy or paraphrase of the text of this security notice 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 1.1	2006-April-21	Added information about Cisco SESM.
Revision 1.0	2005-May-24	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.

Related Information

- **NISCC UK Vulnerability Announcement**
