Cisco Security Advisory

Cisco Unified CallManager and Unified Presence Server ICMP Echo Request Handling Denial of Service Vulnerability

Advisory ID: Cisco-SA-20070328-CVE-2007-1834
Last Updated: 2015 November 25 16:44 GMT
Published: 2007 March 28 17:12 GMT
Version1.1: Final
CVSS Score: Base - 3.3
Workarounds: Yes

CVE-2007-1834
CWE-399

Download CVRF

Download PDF

Email

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

Summary

Cisco Unified CallManager and Unified Presence Server contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

The vulnerability exists due to improper handling of excessive amounts of ICMP echo requests. An attacker could exploit this vulnerability by sending a large number of ICMP echo requests to a CallManager or Presence Server system. These requests may cause various services to crash, resulting in a DoS condition and affecting voice services.

Cisco confirmed this vulnerability in a security advisory and released updates.

Cisco Unified CallManager is the call-processing component of the Cisco IP telephony solution, and the Unified Presence Server is the identity-tracking component of the telephony solution. The vulnerability resides in the way these components handle ICMP echo requests. By sending a large amount of ICMP echo requests to an affected system, attackers can exploit this vulnerability to crash a system, causing a disruption of voice services. This vulnerability can also be exploited by spoofed attacks.

Exploit code is not needed to conduct an attack of this type, which is mainly a brute-force attack. There are many network utility software packages that can aid in the attempted attack, flooding the network and the specific device with ping requests. These utilities can be commercial or open source, making access to them available to anyone who downloads them.

Affected Products

Cisco has released a security advisory for Cisco Bug IDs CSCsg60930 and CSCsf12698 at the following link: cisco-sa-20070328-voip

Vulnerable Products

The following Cisco products are vulnerable:

- Cisco Unified CallManager 5.0 versions prior to 5.0(4a)SU1
- Cisco Unified Presence Server 1.0 versions prior to 1.0(3)

Products Confirmed Not Vulnerable

No other Cisco products are currently known to be affected by these vulnerabilities.

Workarounds

Administrators are advised to apply the appropriate updates.

Administrators may consider blocking ICMP echo requests; however, this will affect network management applications and troubleshooting procedures.

Administrators are advised to put IP telephony systems on an insulated network and to physically secure this network.

The Cisco Applied Intelligence team has created the following companion document to guide administrators in identifying and mitigating attempts to exploit this vulnerability prior to applying updated software: Identifying and Mitigating Exploitation of Multiple Cisco Unified CallManager and Presence Server Vulnerabilities

Fixed Software

Cisco customers with active contracts can obtain updates through the Software Center at the following link: Cisco. Cisco customers without contracts can obtain upgrades by contacting the Cisco Technical Assistance Center at 1-800-553-2447 or 1-408-526-7209 or via e-mail at tac@cisco.com.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20070328-CVE-2007-1834

Revision History

Version	Description	Section	Status	Date
1.1	Updated links to related resources	Multiple	Final	2015-November-25
1.0	Initial release	NA	Final	2007-March-28

Legal Disclaimer