

IP Touch Denial of Service through crafted TFTP request

Summary

A vulnerability has been discovered enabling an attacker to deny audio service from an IP Touch phone set through a specially crafted TFTP request sent to the OmniPCX Enterprise Communication Server. The vulnerability lies actually with the Communication Server.

CVSS V2 Score (base metrics only): 6.8

| | |
|------------------------|------------------|
| Exploitability Metrics | 6.5 |
| Access Vector | Adjacent Network |
| Access Complexity | Low |
| Authentication | None |
| Impact Metrics | 7.8 |
| Confidentiality Impact | Partial |
| Integrity Impact | None |
| Availability Impact | Complete |

History

Date of notification to Alcatel-Lucent: 5 June 2007

Date of notification to Business Partners: 29 June 2007

Date corrective integrated in mainline: 26 July 2007

Date corrective integrated in last product line: 25 October 2007

Date of public advisory creation: 14 November 2007 (Ed.01)

Affected Products and Configurations

OmniPCX Enterprise R7.1 and earlier.

Detailed description

Upon boot, an IP Touch phone downloads configuration information about the deployment using the TFTP protocol.

The attack against a given IP Touch phone set is performed by sending a specially crafted TFTP request containing this phone's MAC address (Ethernet address) faking this initial download request. The Communication Server thereafter considers the attacking PC's IP address as the phone set's IP address for the incoming half of the voice connection.

Because the signaling link is not broken, the phone stays up and can dial and receive calls, without any ring tone and audio feedback. Communications are halfway with only the outgoing audio but no audio is received from the far end.

Impact of the vulnerability

The attacked IP Touch phone set can dial outgoing calls, rings on incoming calls but no audio is heard on the phone. Audio is correctly sent from the attacked IP Touch phone to the other party.

To recover the phone's functionality the phone needs to reconnect to the OmniPCX Enterprise Communication Server. This is easily achieved through a phone power off/power on.



Solutions

Workaround

In installations with IP address spaces for phone sets separate from that of the data workstations, bogus TFTP requests may be filtered using a firewall in front of the Communication Server. The firewall is configured to allow TFTP requests only from the range of IP addresses allocated to IP Touch phones and block any TFTP request coming from other IP addresses, thereby blocking any bogus request emitted from any workstation.

Fixed Software Versions and how to obtain them

Please contact your Business Partner to determine the appropriate course of action. For information the correction has been delivered in the following patches:

- OmniPCX Enterprise R7.1: install patch F5.401.21.e
- OmniPCX Enterprise R7.0: upgrade to release R7.1
- OmniPCX Enterprise R6.2: install patch F3.301.38.a
- OmniPCX Enterprise R6.1: install patch F2.502.33
- OmniPCX Enterprise R6.0 and earlier: those releases are phased out: upgrade to release R7.1.

References

Discoverer reference: Compass Advisory: Alcatel VoIP Phones

CVE entry number: CVE-2007-5361

CERT-IST alert reference: CERT-IST/AV-2007.534

This vulnerability is tracked as Alcatel-Lucent defect number XTScf00923

Vendor Statement

Alcatel-Lucent is committed to continuously enhancing our security posture, and we have both internal and external resources involved in security review processes aimed at identifying product vulnerabilities, both in existing and in developing products.

It is important to note that there have been no reports of compromise due to this vulnerability. Alcatel-Lucent's primary concern in this instance is to rapidly deploy a solution for our entire customer base. As a result, Alcatel-Lucent has released patches for most code versions.

We highly recommend that you upgrade your OmniPCX Enterprise to a patch corresponding to your currently installed release. While we encourage customers to always utilize the latest releases to ensure the full benefit of our continued innovation and improvements, we recognize that this is not always possible.

Information on our disclosure policy, how to report vulnerabilities can be found at <http://www1.alcatel-lucent.com/psirt>.