

Shell injection vulnerability in OmniPCX Enterprise Unified Maintenance Tool

Summary

A vulnerability has been found in the Unified Maintenance Tool shipped with OmniPCX Enterprise. This vulnerability allows the execution under the identity of user `httpd` of shell commands on an OmniPCX Enterprise Communication Server.

CVSS Score (base metrics only) : (including steps how this number was achieved)

CVSS v1 Base score	9.3
Access Vector	Remote
Access Complexity	Low
Authentication	Not Required
Confidentiality Impact	Partial
Integrity Impact	Complete
Availability Impact	Complete
Impact Bias	Weight availability

History

Date of notification : 10 may 2007

Date of creation : Ed.01 (11 September 2007)

Affected Products and Configurations

OmniPCX Enterprise (all releases up to and including R7.1)

Detailed description

The Unified Maintenance Tool is used by maintenance teams to display telephony system internal status information during support operations. This tool, amongst other services, offers through a Web-based interface a way to test the liveness of a given IP address or system name.

One of the CGI script implementing this tool incompletely validates input it receives from the user and lets through shell meta-characters. The input string is passed by the CGI engine to a shell running under the identity of user `httpd`. The incorrectly filtered input is interpreted by this shell, resulting in the vulnerability.

Commands requiring an input stream (for example a command interpreter) will fail.

Impact of the vulnerability

Any user with IP connectivity with the OmniPCX Enterprise Communication Server can run any of the commands available to user `httpd` under this identity. Using this vulnerability, remote Denial of Service can be performed on the telephony service or content disclosure for the files accessible to user `httpd`, or even content alteration of files writable by user `httpd`.

Solutions



Workaround

Please contact your Business Partner to determine the appropriate course of action.

1. Either deactivate the Web server with the `netadmin` command. The following functionalities are lost:
 - File download through HTTP becomes impossible:
 - 4760i lightweight configuration client cannot be downloaded anymore although it can still be used if previously downloaded to the workstation;
 - The OmniTouch Unified Communication application cannot download voice messages from the integrated voice mail anymore;
 - Unified Maintenance Tool (subject of this alert).
2. or if the Web server cannot be deactivated, interpose a firewall in front of the Communication Server to allow access to TCP ports 80 and 443 only from authorized workstations.

Fixed Software Versions and how to obtain them

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

- OmniPCX Enterprise R7.1: install patch F5.401.19 (available week 23)
- OmniPCX Enterprise R7.0: upgrade to release R7.1
- OmniPCX Enterprise R6.2: install patch F3.301.37 (available week 29)
- OmniPCX Enterprise R6.1: install patch F2.502.32 (available week 28)
- OmniPCX Enterprise R6.0 and earlier: those releases are phased out: upgrade to release R7.1.

References

Discoverer reference: RedTeam Pentesting GmbH <http://www.redteam-pentesting.de/advisories/rt-sa-2007-001.php>

CVE entry number: CVE-2007-3010

This vulnerability is tracked as Alcatel-Lucent Enterprise defect number: XTSc99221

Vendor Statement

Alcatel-Lucent is committed to continuously enhance 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 supported code versions.

We highly recommend that you upgrade your OmniPCX Enterprise to the most recent patch corresponding to your currently installed release. While we encourage customers to always utilize the latest release 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>.