CERT Advisory CA-2002-32 Backdoor in Alcatel OmniSwitch AOS

Original release date: November 21, 2002
Last revised: Thu Jan 2 13:02:38 EST 2003
Source: CERT/CC, Alcatel

A complete revision history can be found at the end of this file.

Systems Affected

- Alcatel OmniSwitch 7700/7800 switches running Alcatel Operating System (AOS) version 5.1.1

Overview

Alcatel has recently discovered a serious vulnerability in AOS version 5.1.1. Exploitation of this vulnerability can lead to full administrative control of the device running AOS.

I. Description

AOS typically runs on network infrastructure devices, such as the Alcatel OmniSwitch 7000 series switch. According to Alcatel:

> *During an NMAP audit of the AOS 5.1.1 code that runs on the Alcatel OmniSwitch 7700/7800 LAN switches, it was determined a telnet server was listening on TCP port number 6778. This was used during development to access the Wind River Vx-Works operating system. Due to an oversight, this access was not removed prior to product release.*

Further information about this vulnerability may be found in VU#181721. This issue is also being referenced as CAN-2002-1272:

> *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1272*

II. Impact

An attacker can gain full access to any device running AOS version 5.1.1, which can result in, but is not limited to, unauthorized access, unauthorized monitoring, information leakage, or denial of service.

III. Solution

Upgrade to AOS 5.1.1.R02 or AOS 5.1.1.R03

Contact Alcatel's customer support for the updated AOS.

Workarounds

Block access to port 6778/TCP at your network perimeter.

Appendix A. - Vendor Information

VU#181721 was written by Alcatel. As new vendor information is reported to the CERT/CC, we will update VU#181721 and note the changes in our revision history.

Appendix B. - References

1. VU#181721: Alcatel OmniSwitch 7700/7800 does not require a password for accessing the telnet server - http://www.kb.cert.org/vuls/id/181721
2. OmniSwitch_7000_brief - http://www.ind.alcatel.com/nextgen/OmniSwitch_7000_brief.pdf
3. CAN-2002-1272 - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1272

We thank Olivier Paridaens and Jeff Hayes of Alcatel for reporting this issue.

Author: Ian A. Finlay.

Revision History

November 21, 2002: Initial release
January 02, 2002: Changed URL for Alcatel Customer Support