

[NEWS] Telnet DoS Vulnerability in Marconi ATM Switch

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-09/0028.html>

From: support@securiteam.com

Date: 09/06/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NEWS] Telnet DoS Vulnerability in Marconi ATM Switch

Message-Id: <20010906045137.360C4138C0@mail.der-keiler.de>

Date: Thu, 6 Sep 2001 06:51:37 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Telnet DoS Vulnerability in Marconi ATM Switch

SUMMARY

Marconi ATM switches can be configured with IP addresses for remote administration via telnet and web interfaces. There is a bug that can be used to deny telnet access to the switch. The web interface does not appear vulnerable, and console management is unaffected.

DETAILS

History:

<<http://www.securiteam.com/securitynews/5YP0M0A3FO.html>> Denial of Service against Fore/Marconi ASX Switches

Marconi ForeThought 6.2 had an administrative DoS vulnerability in its TCP/IP. This was fixed by Marconi as of FT6.2.0_1.73390. Newer versions of ForeThought include a second telnet session intended only for administrative users. The idea is that if someone is logged into the switch the second login would be reserved for users with administrative privileges.

Description:

Securiteam: [NEWS] Telnet DoS Vulnerability in Marconi ATM Swit

The upgrade Marconi released did fix the problem with the underlying TCP stack, however there is another higher layer bug that allows both telnet sessions to be locked, completely preventing standard telnet access to the switch. Unfortunately, the vulnerability is such that some port scans may trigger it unintentionally. In addition, there is no way to clear the locked sessions even from a console connection (security telnet kill 0, for example, has no effect). Rebooting the switch is the only known way to make those telnet sessions available again.

Details:

Hardware tested: Marconi ASX-200, P5 cpu

Software version: ForeThought 71.1.0_1.83325.bin

Test software: nmap V. 2.53

Command issued: RPCgrind scan against telnet port (23)

Results: security telnet show->

Will show the User ID as "Logging in..." along with the IP address that connected to the switch. In addition, the idle time will stay at 0s forever, while there is no underlying TCP connection state associated with this session.

Workaround:

Marconi was notified at the end of July. Engineers have found the bug and will have a fixed version available shortly. In the meantime, telnet access to Marconi ASX switches should be allowed only from management networks. The version of ForeThought tested has an IPFilter option that seems a viable workaround (security ipf). It appears to drop any packet destined for an internal IP on the switch that is not sourced from a host or network listed in the IPF rules.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:anub-securityfocus@open.mine.nu> Christopher Kruslicky.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

Securiteam: [NEWS] Telnet DoS Vulnerability in Marconi ATM Swit

- **Previous message:** support@securiteam.com: "[\[UNIX\] Gauntlet Firewall for UNIX and WebShield CSMAP and smap/smapd Buffer Overflow Vulnerabilities](#)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)