

[UNIX] AFTPd Core Dump Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0048.html>

From: support@securiteam.com

Date: 01/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 12 Jan 2002 10:46:26 +0100 (CET)

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.

AFTPd Core Dump Vulnerability

SUMMARY

When a vulnerable version of AFTPd is used under FreeBSD, other systems might be also affected (AFTPd is not the official FreeBSD FTP server), it is possible to cause the program to core dump the memory by issuing a special FTP change directory command. If the authentication mechanism is accessed prior to the core dump, the password file will be found inside the core dump.

DETAILS

Vulnerable systems:

AFTPd version 5.4.4 and prior

Issuing an authentication request (doesn't have to be a valid one) followed by the command: "cd ~" will cause the FTP server to crash, dumping the memory file into the currently accessed directory. The core dump will include the password file the FTP server has just accessed in order to authenticate the user.

ADDITIONAL INFORMATION

The information has been provided by <mailto:nu_omega_tau@altavista.com>
Nu Omega Tau.

Securiteam: [UNIX] AFTPd Core Dump Vulnerability

=====

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.

-
- **Previous message:** support@securiteam.com: "[REVS] E-mail Spoofing and CDONTS.NEWMAIL (Protecting Microsoft Active Server Pages Applications)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)