

[NT] Multiple Windows-Based FTP Servers Vulnerable to DoS under Windows 98

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0024.html>

From: support@securiteam.com

Date: 08/02/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [NT] Multiple Windows-Based FTP Servers Vulnerable to DoS under Windows 98

Message-Id: <20010802053711.381E313901@mail.der-keiler.de>

Date: Thu, 2 Aug 2001 07:37:11 +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>

Multiple Windows-Based FTP Servers Vulnerable to DoS under Windows 98

SUMMARY

Several FTP server products running under Windows 98 (first edition) with the 'CON\CON' kernel patch by Microsoft are vulnerable to a security weakness that allows remote attackers to cause the program crash, bringing down the whole operating system ("Blue screen of death").

DETAILS

Vulnerable systems:

BisonFTP version 4R1

Broker FTP Server version 5.9.5.0

G6 FTP Server version 2.15 (a.k.a. Bulletproof FTP Server)

GuildFTPD version 0.922

SurgeFTP version 2.0f

WarFTPD version 1.71

WFTPD version 3.00 R5

Immune systems:

ArGoSoft FTP Server version 1.2.2.2

Serv-U FTP Server version 3.0

Issuing a GET command with a DOS device name to the above vulnerable servers, causes the products to strange behavior from consuming 100% CPU time to completely crashing the computer.

Hypermail Development List: [NT] Multiple Windows-Based FTP Ser

Some FTP servers have filtering algorithms to prevent issuing a GET for the 'AUX' device, but this filtering can easily be circumvented by referring to the device as 'AUX.' (with a trailing dot).

ADDITIONAL INFORMATION

The information has been provided by <mailto:byterage@yahoo.com>
ByteRage.

=====

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.

-
- *Next message:* support@securiteam.com: "[UNIX] Linux Kernel IP Masquerading Vulnerability"
 - *Previous message:* support@securiteam.com: "[NT] 1st Choice FTPPro Stores Passwords Insecurely"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)