## 164.115.32.57

### Scan Information

| | |
|---|---|
| Start time: | Fri Sep 13 01:13:40 2013 |
| End time: | Fri Sep 13 01:34:36 2013 |

### Host Information

| | |
|---|---|
| IP: | 164.115.32.57 |
| OS: | Microsoft Windows Vista, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows 7 |

### Results Summary

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 2 | 0 | 0 | 0 | 2 |

### Results Details

#### 80/tcp

67260 - PHP 5.4.x < 5.4.17 Buffer Overflow [-/+]

### Synopsis

The remote web server uses a version of PHP that is potentially affected by a buffer overflow vulnerability.

### Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.17. It is, therefore, potentially affected by a buffer overflow error that exists in the function '_pdo_pgsql_error' in the file 'ext/pdo_pgsql/pgsql_driver.c'.

Note that this plugin does not attempt to exploit this vulnerability, but instead, relies only on PHP's self-reported version number.

### See Also

http://bugs.php.net/64949

http://www.php.net/ChangeLog-5.php#5.4.17

## Solution

Apply the vendor patch or upgrade to PHP version 5.4.17 or later.

## Risk Factor

High

## CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## Plugin Information:

Publication date: 2013/07/12, Modification date: 2013/07/12

## Ports

### tcp/80

```
Version source : Server: Apache/2.4.4 (Win32) PHP/5.4.16
Installed version : 5.4.16
Fixed version : 5.4.17
```

69401 - PHP 5.4.x < 5.4.18 Multiple Vulnerabilities [-/+]

## Synopsis

The remote web server uses a version of PHP that is potentially affected by multiple vulnerabilities.

## Description

According to its banner, the version of PHP 5.4.x installed on the remote host is a version prior to 5.4.18. It is, therefore, potentially affected by the following vulnerabilities :

- A heap corruption error exists in numerous functions in the file 'ext/xml/xml.c'. (CVE-2013-4113 / Bug #65236)

- An error exists related to certificate validation, the 'subjectAltName' field and certificates containing NULL bytes. This error can allow spoofing attacks.
(CVE-2013-4248)

Note that this plugin does not attempt to exploit these vulnerabilities, but instead, relies only on PHP's self-reported version number.

## See Also

http://bugs.php.net/65236

http://www.php.net/ChangeLog-5.php#5.4.18

## Solution

Upgrade to PHP version 5.4.19 or later.

Note the 5.4.18 release contains an uninitialized memory read bug and a compile error that prevent proper operation.

## Risk Factor

High

## CVSS Base Score

9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## CVSS Temporal Score

7.7 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

## STIG Severity

I

## References

| | |
|---|---|
| BID | 61128 |
| BID | 61776 |
| CVE | CVE-2013-4113 |
| CVE | CVE-2013-4248 |
| XREF | OSVDB:95152 |
| XREF | OSVDB:96298 |
| XREF | IAVB:2013-B-0093 |

## Plugin Information:

Publication date: 2013/08/21, Modification date: 2013/08/27

## Ports

**tcp/80**

```
Version source : Server: Apache/2.4.4 (Win32) PHP/5.4.16
Installed version : 5.4.16
Fixed version : 5.4.18
```