PHP: Supplement

# Notes and References

The major release dates for PHP are

* 5.3.0: June 2009
* 5.4.0: March 2012
* 5.5.0: June 2013
* 5.6.0: August 2014
* 7.0.0: December 2015
* 7.1.0: December 2016
* 7.2.0: November 2017

Source: <http://php.net/releases/>.

Table 20-1. Default included version of PHP, by Linux distribution

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| CentOS |  |  | Mint |  |  | 13.1 | 5.4.20 |
| 7.4.1708 | 5.4.16-42 |  | 18.3 | 7.0.30 |  | 12.3 | 5.3.17 |
| 7.3.1611 | 5.4.16-42 |  | 18.2 | 7.0.30 |  | 12.2 | 5.3.15 |
| 7.2.1511 | 5.4.16-36 |  | 18.1 | 7.0.4 |  | 12.1 | 5.3.8 |
| 7.1.1503 | 5.4.16-23 |  | 18 | 7.0.4 |  | 11.4 | 5.3.5 |
| 7.0.1406 | 5.4.16-21 |  | 17.3 | 5.5.9 |  | Ubuntu |  |
| 6.8 | 5.3.3-49 |  | 17.2 | 5.5.9 |  | 17.10 | 7.1.8 |
| 6.7 | 5.3.3.-47 |  | 17.1 | 5.5.9 |  | 17.04 | 7.0.15 |
| 6.6 | 5.3.3-40 |  | 17 | 5.5.9 |  | 16.10 | 7.0.8 |
| 6.5 | 5.3.3-38 |  | 16 | 5.5.3 |  | 16.04 | 7.0.4 |
| 6.4 | 5.3.3-26 |  | 15 | 5.4.9 |  | 15.10 | 5.6.11 |
| 6.3 | 5.3.3-22 |  | 14 | 5.4.6 |  | 15.04 | 5.6.4 |
| 6.2 | 5.3.3-3 |  | 13 | 5.3.10 |  | 14.10 | 5.5.12 |
| 6.1 | 5.3.3-3 |  | 12 | 5.3.6 |  | 14.04 | 5.5.9 |
| 6.0 | 5.3.3-3 |  | 11 | 5.3.5 |  | 13.10 | 5.5.3 |
| 5.11 | 5.3.2-6 |  | 10 | 5.3.3 |  | 13.04 | 5.4.9 |
| 5.10 | 5.1.6-40 |  | OpenSuSE |  |  | 12.10 | 5.4.6 |
| 5.9 | 5.1.6-39 |  | 42.3 | 5.5.14/7.0.7 |  | 12.04 | 5.3.10 |
| 5.8 | 5.1.6-32 |  | 42.2 | 5.5.14/7.0.7 |  | 11.10 | 5.3.6 |
| 5.7 | 5.1.6-27 |  | 42.1 | 5.5.14 |  | 11.04 | 5.3.5 |
| 5.6 | 5.1.6-27 |  | 13.2 | 5.6.1 |  |  |  |

Table 20-2 Selected release dates and included versions of Apache, MySQL/MariaDB and PHP for XAMPP between 2011 and 2017. Source: http://xampp.wikia.com/wiki/XAMPP\_for\_Windows/Versions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| XAMPP | Apache | MySQL/MariaDB | PHP | Release |
| 7.2.0 |  |  | 7.2.0 | 12/20/2017 |
| 7.1.1 | 2.4.25 | 10.1.21 | 7.1.1 | 2/1/2017 |
| 7.0.15 | 2.4.25 | 10.1.21 | 7.0.15 | 2/1/2017 |
| 7.0.13 | 2.4.23 | 10.1.19 | 7.0.13 | 11/18/2016 |
| 7.0.9 | 2.4.23 | 10.1.16 | 7.0.9 | 8/31/2016 |
| 7.0.8 | 2.4.18 | 10.1.13 | 7.0.8 | 6/28/2016 |
| 7.0.6 | 2.4.18 | 10.1.13 | 7.0.6 | 5/12/2016 |
| 7.0.5 | 2.4.18 | 10.1.13 | 7.0.5 | 4/21/2016 |
| 7.0.4 | 2.4.18 | 10.1.10 | 7.0.4 | 3/4/2016 |
| 7.0.3 | 2.4.18 | 10.1.10 | 7.0.3 | 2/19/2016 |
| 7.0.2 | 2.4.18 | 10.1.10 | 7.0.2 | 1/29/2016 |
| 7.0.1 | 2.4.18 | 10.1.9 | 7.0.1 | 12/31/2015 |
| 7.0.0 | 2.4.18 | 10.1.9 | 7.0.0 | 12/23/2015 |
| 7.0.0 | 2.4.18 | 10.1.9 | 7.0.0 | 12/23/2015 |
| 5.6.3 | 2.4.10 | 5.6.21 | 5.6.3 | 11/19/2014 |
| 5.5.19 | 2.4.10 | 5.6.21 | 5.5.19 | 11/19/2014 |
| 1.8.3-0 | 2.4.4 | 5.6.11 | 5.5.1 | 7/29/2013 |
| 1.8.2-0 | 2.4.4 | 5.5.32 | 5.4.16 | 6/26/2013 |
| 1.8.1 | 2.4.3 | 5.5.27 | 5.4.7 | 9/29/2012 |
| 1.8.0 | 2.4.2 | 5.5.25a | 5.4.4 | 7/13/2012 |
| 1.7.7 | 2.2.21 | 5.5.16 | 5.3.8 | 9/20/2011 |
| 1.7.5 | 2.2.21 | 5.5.15 | 5.3.8 | 9/14/2011 |
| 1.7.4 | 2.2.17 | 5.5.8 | 5.3.5 | 1/22/2011 |

The Windows Cache Extension for PHP is a tool to speed up PHP applications running on Windows Server. The extension is available for download from <https://sourceforge.net/projects/wincache/>. For documentation on the extension, see <https://www.iis.net/downloads/microsoft/wincache-extension>.

Exercises

1. When configuring PHP to run as a CGI script, the text suggests setting the options +ExecCGI +FollowSymLinks on the directory /usr/bin. What are the security implications? Suggest a better alternative.
2. Install XAMPP on a Windows system. Use the passwords page (http://localhost/security/xamppsecurity.php) to update the password for the XAMPP status page. View the file C:\xampp\htdocs\xampp\.htaccess. Determine the authentication mechanism XAMPP uses and find the file that contains the credentials. What hashing algorithm is used? Is it reasonable?
3. Run the remote include attack manually, setting up a netcat listener and using the Kali web shell /usr/share/webshells/php/php-reverse-shell.php. Is it possible to evade ModSecurity by URL encoding the data in the request? What about double URL encoding the data in the request?
4. Verify that the Metasploit remote include attack also works if the target is running PHP on Windows using XAMPP.
5. Verify that the Metasploit remote include attack also works if the target is running PHP on Windows using IIS. Does ModSecurity on Windows block the attack?
6. Capture the network traffic between Weevely and an agent. Is the traffic encrypted?
7. Modify the PHP persistence malware to call back to the user that requested it on a port specified in a get request.