

STATEMENT

Statement regarding PSM and PHP Vulnerabilities

Document Date: 2026-10-21

PSM is an application which is programmed in PHP, and therefore is also a candidate for vulnerabilities.

As of today, 21st of October, it has become known that there are two security bulletins related to PHP.

See PHP: News Archive - 2026 <https://www.php.net/archive/2026.php#2026-10-20-1> for more information.

1

PHP Security Bulletins

- **RCE via OOM corruption, CVE-2026-109618 (GHSA-w8hw-w9fx-j79w):** out-of-memory handling can interrupt PHP while internal request data is only partially initialized. Request cleanup may then treat the invalid data as valid.
- **RCE via stale global state, CVE-2026-109619 (GHSA-6wmf-4rv5-p3rp):** request-owned internal state can survive after its backing memory has been freed. A later request handled by the same worker may use that stale state before normal initialization resets it.

NOTE

The vulnerabilities are especially critical in environments that can be accessed from the internet. PSM is normally installed in the internal network, and it cannot be accessed from the internet.

2 Planned Steps and Preparation

Statement regarding our planned steps, and things you can already prepare:

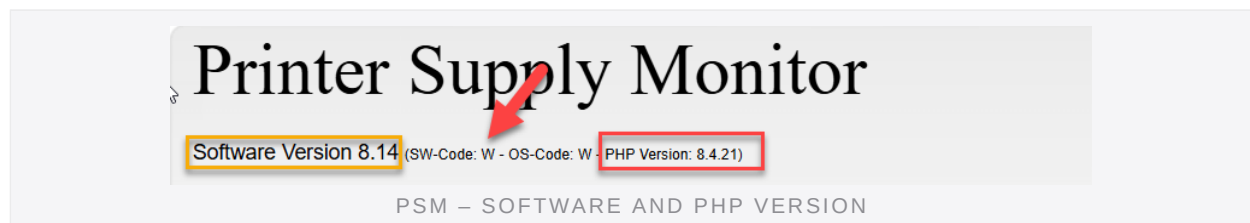
As the updated patches for PSM are just about to become available, we need to do some actions and testing ourselves, before we can release new packages.

Since PSM is in all known cases installed in the intranet only, and cannot be accessed from the internet, the risk is limited. The vulnerabilities could only be used by people within your own network. We recommend limiting access to the web server, which has a connection to PHP, to the workstations which need to have access to it.

- If your PSM is running on a Windows Server, use your firewall to block access to port 80/443 of that server using the internal Windows Firewall. Or – in larger networks – limit access to port 80/443 to the workstations, which need to have access to PSM.
- Raspberry Pi Boxes: limit access to port 80/443 to the workstations, which need to have access to PSM.

3 Identify Your PSM Version

- Identify the current version of PSM you have. This is shown after you log in to PSM. In the example below, you will see that your PSM is running PHP 8.4.x



Prepare for the work to be done, depending on the version you have

4 SW-Code: W – PHP Version 8.4.xx

- Software Version 8.14. This is the most current version of PSM. If you have a lower level, you can update using the image here:
 - <https://partner.sysprint.ch/filegator/repository/PSM-Patches/Windows-PHP84-V8.1.4PSM.zip>
- SW-Code: W means that you have PSM Windows.
- PHP Version 8.4.xx means that you have a PHP version which will be patched.

Expect the following, once the patch is made available by us:

- Uninstall the PHP version from the server
- Reinstall the new PHP version on the server

5 SW-Code: W – PHP Version 8.1.xx

- Software Version 8.14. This is the most current version of PSM. If you have a lower level, you can update using the image here:
 - <https://partner.sysprint.ch/filegator/repository/PSM-Patches/Windows-PHP8-V8.1.4PSM.zip>
- SW-Code: W means that you have PSM Windows.
- PHP Version 8.1.xx means that you have a PHP version which cannot be patched, it will require a new installation.

Expect the following, once the patch is made available by us:

- Make sure that the current PSM version 8.14 is installed
- Back up PSM via the web GUI
- Uninstall modules belonging to PSM:
 - PSM
 - PHP
 - MySQL
- Reinstall the most current package which we will publish

6

SW-Code: W – PHP Version 7.3.xx

- Software Version 8.14. This is the most current version of PSM. If you have a lower level, you can update using the image here:
 - <https://partner.sysprint.ch/filegator/repository/PSM-Patches/Windows-PHP7-V8.1.4PSM.zip>
- SW-Code: W means that you have PSM Windows.
- PHP Version 7.3.xx means that you have a PHP version which cannot be patched, it will require a new installation.

Expect the following, once the patch is made available by us:

- Make sure that the current PSM version 8.14 is installed
- Back up PSM via the web GUI
- Uninstall modules belonging to PSM:
 - PSM
 - PHP
 - MySQL
- Reinstall the most current package which we will publish

7

SW-Code: W – PHP Version 5.6

- Software Version 8.14. This is the most current version of PSM. If you have a lower level, you can update using the image here:
 - <https://partner.sysprint.ch/filegator/repository/PSM-Patches/V8.1.4PSM.zip>
- SW-Code: W means that you have PSM Windows.
- PHP Version 5.xx.xx means that you have a PHP version which cannot be patched, it will require a new installation.

Expect the following, once the patch is made available by us:

- Make sure that the current PSM version 8.14 is installed
- Back up PSM via the web GUI
- Uninstall modules belonging to PSM:
 - PSM
 - PHP
 - MySQL
- Reinstall the most current package which we will publish

8**Raspberry Pi Boxes**

Bad news. All PHP boxes out in the field are using PHP versions which cannot be patched anymore.

We will have to build a complete new image for the flash card installed in your Raspberry box. This will take some time. We recommend restricting network access to port 80 and 443 as described earlier.