

"PHP2Shell" Advisory

Publication date: 2026 October 26

This document aims to provide information on the assessment of a potential product impact linked with the recently disclosed set of vulnerabilities "PHP2Shell".

Executive Summary

As detailed in the following [ENISA joint statement](#) and [CISA Advisory](#), 2 vulnerabilities have been found in PHP. The [EUVD-2026-107260 / CVE-2026-109618 \(GHSA-w8hw-w9fx-j79w\)](#) and [EUVD-2026-107265 / CVE-2026-109619 \(GHSA-6wmf-4rv5-p3rp\)](#) show an overall CVSSv4.0 score of 9.2 which is considered Critical.

These vulnerabilities concern software products that rely on affected versions of PHP to provide web-based interfaces, applications, or network-accessible services. Such products may be impacted if vulnerable PHP components are present.

PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE).

PHP uses `longjmp()` for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE).

These vulnerabilities may affect products relying on vulnerable PHP versions, potentially compromising the confidentiality, integrity, and availability of affected systems.

Type of the vulnerabilities:

- **Remote code execution (RCE),**
- **Unauthorized access to sensitive information,**
- **Data modification or theft,**
- **Denial-of-service (DoS) conditions**

Fresenius is actively monitoring “PHP2Shell”, and analyses have been initiated to determine whether any of our current products are impacted.

Fresenius products assessment

The following list of products were assessed and **are not affected by “PHP2Shell”**.

Fresenius Kabi

Infusion & Nutrition Systems

Product	Versions
Agilia Link (V2)	All versions
Agilia Link+ (V2)	All versions
Agilia MRI Guard (V2)	All versions
Agilia Partner (V2)	All versions
Agilia Proneo (V2)	All versions
Agilia SP (V2)	All versions
Agilia SP MC (V2)	All versions
Agilia SP MC US (V2)	All versions
Agilia SP PCA (V2)	All versions
Agilia SP Tiva (V2)	All versions
Agilia VP (V2)	All versions
Agilia VP MC (V2)	All versions
Agilia VP MC US (V2)	All versions
Ambix nova	All versions
Amika	All versions
Amika and Ambix nova Partner	All versions
Amika JP	All versions
Amika V JP	All versions
Amika+	All versions
APPLIX SMART	All versions
APPLIX VISION	All versions
Centerium	All versions
Conox	All versions
Conox - 2D	All versions
Conox Bridge	All versions
Conox Lite	All versions

Conox View PC	All versions
Exelia Combox	All versions
Exelia Link	All versions
Exelia Partner	All versions
Exelia SP	All versions
Exelia Therapy Manager	All versions
Exelia VP	All versions
INfusio Centro	All versions
INfusio DC7	All versions
INfusio DC7 WiFi	All versions
INfusio DC7s	All versions
INfusio DC7s WiFi	All versions
INfusio Helper	All versions
INfusio SP(SP7s-V5)	All versions
INfusio VP(VP7s-V5)	All versions
Injectomat Agilia	All versions
Injectomat MC Agilia (V1)	All versions
Injectomat Tiva Agilia (V1)	All versions
Ivenix IMS Software	All versions
Ivenix LVP Software	All versions
Link Agilia (V1)	All versions
Link+ Agilia (V1)	All versions
MRI Guard Agilia (V1)	All versions
Optima	All versions
Orchestra DPS	All versions
Orchestra MVP	All versions
Orchestra Stations	All versions
Partner Agilia (V1)	All versions
Partner Agilia US (V1)	All versions
ProNeo Agilia (V1)	All versions
Sentinel standalone	All versions
Vigilant Software Suite 1	All versions
Vigilant Software Suite 2	All versions
Vigilant Software Suite US	All versions
VMM Device Uploader	All versions
Volumat Agilia (V1)	All versions
Volumat MC Agilia (V1)	All versions
Volumat MC Agilia US (V1)	All versions

Transfusion Medicine & Cell Therapies

Product	Versions
Alyx	All versions
AmiCORE	All versions
Amicus LE	All versions
Amicus Legacy	All versions
Aurora	All versions
Aurora Xi	All versions
CATSmart	All versions
CompoDock	All versions
CompoGuard Advance	All versions
Compoguard Plus	All versions
CompoMaster G5 Plus	All versions
CompoMat G5 Plus	All versions
COMTEC	All versions
Cue	All versions
Cue Desktop Application	All versions
DockMaster	All versions
DonationMaster _Net	All versions
DonationMaster Advance	All versions
DXT	All versions
Lovo	All versions
Phelix	All versions

Compounding Devices

Product	Versions
KabiHelp Assist® Pro	All versions
KabiHelp® Pro	All versions

“PHP2Shell” impact rationale

The afore-mentioned products do not rely on PHP.

None of “PHP2Shell” reported vulnerabilities can be exploited on these products.

The following vulnerabilities are associated with “PHP2Shell”:

1. [EUVD-2026-107260](#) / [CVE-2026-109618](#)
2. [EUVD-2026-107265](#) / [CVE-2026-109619](#)

General Cybersecurity recommendations

Proper cybersecurity hygiene and behavior is required to safely integrate Medical Devices into IT infrastructure. The Fresenius Group recommends operators of Medical Devices and software to incorporate the following industry best practices into their defense-in-depth strategy:

- Conduct a comprehensive and periodic security risk assessment on the medical network in accordance with operational security best practices such as ISO 27002
- Minimize network exposure for all medical devices and systems, and ensure that they are not accessible from the Internet
- Locate Fresenius Medical Devices behind firewalls, in dedicated medical networks, isolated from all other IT networks
- Monitor and control access and traffic to the dedicated medical network
- Implement application firewalls capable of deep packet inspection to help protect against zero-day vulnerabilities and the latest exploits
- Use appropriate authentication and authorization of users on the network
- Implement physical controls that ensure no unauthorized persons would have access to the medical devices and systems
- Ensure that all programming software and equipment (service laptops, etc.) are kept in locked cabinets and are never connected to any network other than the medical network they are intended to service
- Ensure that all portable media used for data exchange with the medical network (such as CDs, USB drives, etc.) are scanned before use
- Implement a process to monitor, prevent and contain malware and computer viruses.

Institutionalizing strong cybersecurity policies and following the industry best practices relative to IT security could minimize exposure to threats. These threats may include but not limited to: Data Leak, Data Corruption, Data Loss, Network or Service Outage, etc.

References

Regarding “PHP2Shell” more details can be found on:

PHP Security Advisories:

<https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>

<https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>

CERT-EU Security Advisory:

<https://cert.europa.eu/publications/security-advisories/2026-018/>

NVD Advisories:

[NVD-CVE-2026-109618](#)

[NVD-CVE-2026-109619](#)

MITRE:

[CVE Record: CVE-2026-109618](#)

[CVE Record: CVE-2026-109619](#)

ENISA Statement:

<https://www.enisa.europa.eu/news/joint-statement-on-critical-php-vulnerabilities>

CISA Cybersecurity Advisory:

<https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching>

Contacts

For any questions or suggestions please contact your regional marketing manager.