

Information 13-2026

Kritische PHP-Sicherheitslücken („PHP2Shell“)

Handlungsempfehlung für Rufanlagen mit **Famalux-/FL-Software**

Am 21.10.2026 hat das PHP-Projekt Sicherheitsupdates für zwei kritische Schwachstellen veröffentlicht (CVE-2026-109618 und CVE-2026-109619, auch „PHP2Shell“ genannt) [1]. Die Lücken haben weltweit zu Warnungen und zu vorsorglichen Abschaltungen von Webseiten geführt [2]. Das BSI hat sie mit der Warnstufe 3/Orange bewertet: Maßnahmen müssen unverzüglich ergriffen werden [3].

Was bedeutet das für Ihre Rufanlage?

Die **Rufdokumentation** der **Famalux-/FL-Software** läuft auf XAMPP mit PHP 7.3.9. Updates des PHP-Projekts gibt es nur für PHP 8.2 und neuer. Ältere Versionen erhalten keine Korrektur und sind als verwundbar zu betrachten [1]. PHP 7.3 wird bereits seit dem 06.12.2021 nicht mehr gepflegt. Die Schwachstellen können es Angreifern ermöglichen, ohne Anmeldung Schadcode auf dem Server auszuführen. Technische Details sind bereits öffentlich, Angriffe sind zu erwarten [3].

Wie hoch ist das Risiko?

Ist die Rufdokumentation von außen erreichbar, zum Beispiel durch eine Portfreigabe im Router oder in der Firewall, besteht akute Gefahr. Das BSI empfiehlt, Systeme ohne Patch notfalls vorübergehend vom Internet zu trennen [3]. Ist sie nur im internen Netzwerk erreichbar, ist das Risiko geringer. Auch dann kann der Rechner nach einem Einbruch an anderer Stelle im Netzwerk angegriffen werden. Dieser Rechner kann zugleich der Server Ihrer Rufanlage sein.

Unsere Empfehlung

- Prüfen Sie umgehend, ob die Rufdokumentation von außen erreichbar ist, und schließen Sie eine solche Freigabe unverzüglich.
- Falls ein externer Zugriff zwingend nötig ist, sollte er nur über ein VPN erfolgen. Beobachten Sie die betroffenen Rechner auf Auffälligkeiten und informieren Sie bei Verdacht Ihre IT-Abteilung.
- **Für eine dauerhafte Lösung empfehlen wir die Migration auf ZELO Config 2025. Diese Software benötigt weder XAMPP noch die betroffene PHP-Version, die beschriebenen Schwachstellen bestehen dort nicht.**

Für den Umstieg auf ZELO Config 2025 sprechen Sie bitte Ihren Servicepartner an, der Sie betreut. Er berät Sie gerne zum Vorgehen und zu den passenden Maßnahmen.

Quellen:

[1] PHP-Projekt, Security Advisory CVE-2026-109618, veröffentlicht am 21.10.2026 (github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w)

[2] tagesschau.de, Bericht zur PHP-Sicherheitslücke ([tagesschau.de/wirtschaft/digitales/php-panne-100.html](https://www.tagesschau.de/wirtschaft/digitales/php-panne-100.html))

[3] BSI, IT-Sicherheitshinweis „PHP: Kritische Schwachstellen bedrohen Webanwendungen weltweit“ (BITS-H 2026-297981-1032), 21.10.2026 ([bsi.bund.de](https://www.bsi.bund.de))

Lüdenscheid, den 23.10.2026



i.A. Benjamin Knoch