Mobile Easykey GmbH · Max-Planck-Str. 11 · 61381 Friedrichsdorf

An unsere Kunden und Partner

Kundendienst Help Desk
Hotline +49 6172 95 66 92
E-Mail khd@mobileeasykey.de
Datum 05.11.2026

Stellungnahme zu den PHP-Sicherheitslücken „PHP2Shell“ (CVE-2026-109618 und CVE-2026-109619)

Sehr geehrte Damen und Herren,

seit dem 20. Oktober 2026 warnen das PHP-Projekt, das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie internationale Sicherheitsbehörden vor zwei kritischen Schwachstellen in der Skriptsprache PHP, die unter dem Namen „PHP2Shell“ bekannt geworden sind. Beide Lücken sind mit einem CVSS-Wert von 9,2 als kritisch eingestuft, erlauben unter bestimmten Bedingungen das Ausführen von Schadcode ohne Anmeldung und werden inzwischen aktiv ausgenutzt.

Die Sicherheit Ihrer Daten und Systeme hat für uns höchste Priorität. Daher informieren wir Sie proaktiv und transparent über den Einsatz von PHP bei Mobile Easykey und unsere Bewertung der Lage.

1. Einsatz von PHP bei Mobile Easykey

PHP spielt in unserer Systemlandschaft nur eine untergeordnete Rolle und kommt ausschließlich an den folgenden zwei Stellen zum Einsatz:

System	Betrieb	PHP-Version	Status PHP2Shell
Lizenzierungsplattform für den Mobile Easykey Manager (MEKM)	Mobile Easykey	**8.3.36**	abgesichert
Webserver eines Zulieferers	Zulieferer	**8.5.12**	abgesichert

2. Bewertung der eingesetzten Versionen

Das PHP-Projekt hat die beiden Schwachstellen am 21. Oktober 2026 mit den Sicherheitsreleases **8.5.12, 8.4.27, 8.3.36 und 8.2.35** geschlossen. Alle älteren Versionen der jeweiligen Versionszweige sind betroffen; PHP 8.1 und älter erhalten keine Korrektur mehr.

Die bei Mobile Easykey bzw. unserem Zulieferer eingesetzten Versionen **PHP 8.3.36** und **PHP 8.5.12** sind genau diese abgesicherten Releases. Beide Systeme enthalten damit die offiziellen Korrekturen für CVE-2026-109618 und CVE-2026-109619 und sind für diese Schwachstellen **nicht angreifbar**.

Zudem befinden sich beide Versionszweige im offiziellen Support des PHP-Projekts (bis jeweils 31.12.2027) und erhalten weiterhin Sicherheitsupdates.

3. Ergänzender Hinweis zu CVE-2026-115560

Am 23. Oktober 2026 hat das PHP-Projekt auf eine weitere, deutlich enger begrenzte Schwachstelle (CVE-2026-115560) hingewiesen, die durch die Releases vom 21. Oktober noch nicht behoben wird. Sie ist nur bei einer seltenen Kombination aus Konfiguration und Anwendungscode ausnutzbar; eine Ausnutzung ist bislang nicht bekannt. Bis zur Korrektur im nächsten regulären Release empfiehlt das PHP-Projekt, die Funktion „session.upload_progress“ zu deaktivieren. Diese Empfehlung ist auf beiden genannten Systemen umgesetzt. Das angekündigte Release werden wir nach Veröffentlichung zeitnah einspielen bzw. bei unserem Zulieferer einfordern.

4. Fazit

Die bei Mobile Easykey eingesetzten PHP-Versionen sind auf dem aktuellen, abgesicherten Stand. Für die als „PHP2Shell“ bekannten Schwachstellen besteht kein Handlungsbedarf, und Auswirkungen auf Ihre Systeme oder den Betrieb unserer Lösungen sind nicht zu erwarten. Wir beobachten die Entwicklung weiterhin aufmerksam und informieren Sie, falls sich an dieser Bewertung etwas ändert.

Für Rückfragen steht Ihnen unser Kundendienst gerne zur Verfügung: telefonisch über die Hotline **+49 6172 95 66 92** oder per E-Mail an **khd@mobileeasykey.de**.

Mit freundlichen Grüßen

Sascha Schmittel
Head of Customer Service
Mobile Easykey GmbH

Quellen: PHP Security Advisories zu CVE-2026-109618 / CVE-2026-109619 (21.10.2026) und CVE-2026-115560 (23.10.2026); BSI-Cybersicherheitswarnung 2026-297981-1032; CISA Known Exploited Vulnerabilities Catalog (Aufnahme am 26.10.2026).