

Gravierende Sicherheitslücke bedroht weltweit Webseiten – auch in Luxemburg

Blogs, Onlineshops und Nachrichtenportale könnten ins Visier von Angreifern geraten. Die PHP-Lücke ermöglicht die Übernahme ganzer Server. Auch im Großherzogtum sind deshalb die Websites einiger Institutionen nicht abrufbar

Von dpa, Uwe Hentschel, Nathalie Roden und
Tiago Teixeira Rodrigues

Wer zurzeit einen Blick auf die Websites des großherzoglichen Hofes, der Chamber, der Finanzaufsicht (CSSF), der Luxtram, der Hôpitaux Robert Schuman, des Luxembourg Institute of Science and Technology (LIST), CSV oder auch der Rockhal werfen möchte, wird sich gedulden müssen. All diese Websites sind vorübergehend nicht verfügbar, nachdem Sicherheitslücken identifiziert wurden, die mehrere Plattformen auf internationaler Ebene betreffen.

In einer Mitteilung, die in den sozialen Netzwerken veröffentlicht wurde, erklärt die Rockhal, dass die vorsorgliche Abschaltung dazu dient, die notwendigen Sicherheitsupdates umzusetzen.

Gefährlicher Fehler ermöglicht vollständige Übernahme

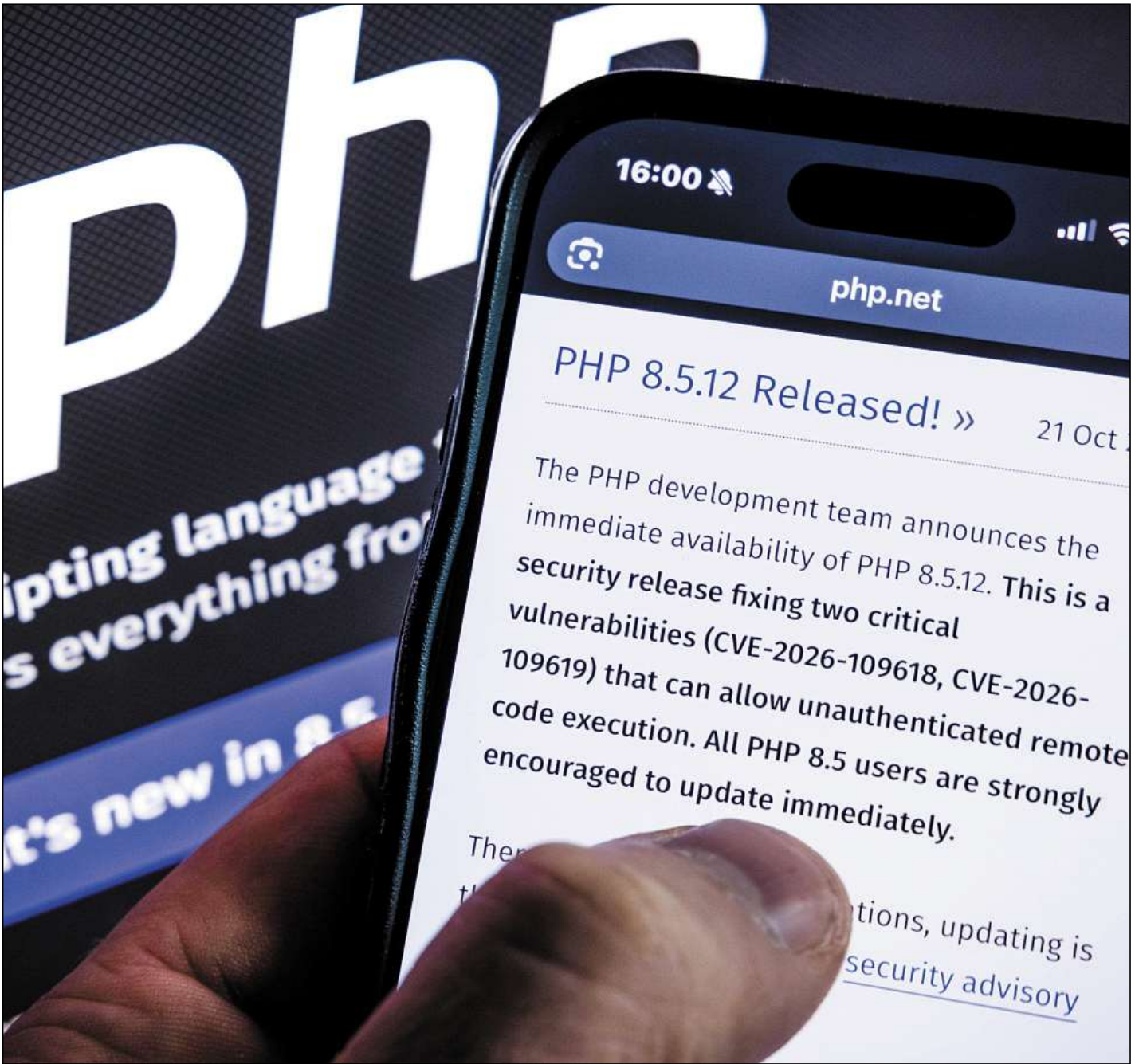
Eine neu entdeckte, schwerwiegende Sicherheitslücke bringt weltweit das Fundament zahlreicher Webseiten und Onlinedienste ins Wanken. Betroffen ist die weit verbreitete Programmiersprache PHP, auf der ein Großteil des gesamten Internets basiert – von einfachen Blogs über große Nachrichtenportale bis hin zu komplexen Onlineshops und Content-Management-Systemen wie WordPress.

Wie unter anderem das IT-Sicherheitsunternehmen Huntress, sowie das offizielle PHP-Sicherheitsteam berichten, handelt es sich um eine akute Notfallsituation, die Betreiber von Internetseiten in aller Welt zu schnellem Handeln zwingt.

- *Angesichts dieser Situation haben die luxemburgischen Behörden mehrere vorbeugende Maßnahmen ergriffen, um das Risiko zu mindern und den Schutz der potenziell betroffenen Systeme zu verstärken.*

Arbeitsgruppe zur Bewertung von Cyberrisiken (CERC)

Auch die luxemburgische Arbeitsgruppe zur Bewertung von Cyberrisiken (CERC), die angesichts der aktuellen Gefahrenlage am Mittwoch tagte, bestätigt, dass nach den derzeit verfügbaren Informationen die Sicherheitslücken von kriminellen Akteuren ausgenutzt werden können. „Angesichts dieser Situation haben die luxemburgischen Behörden mehrere vorbeugende Maßnahmen ergriffen, um das Risiko zu mindern und den Schutz der potenziell betroffenen Systeme zu verstärken“, so die Arbeitsgruppe in einer Mitteilung. Die Behörden arbeiten demnach weiter an einer technischen Analyse.



Eine neu entdeckte, schwerwiegende Sicherheitslücke bringt weltweit das Fundament zahlreicher Webseiten und Onlinedienste ins Wanken. Betroffen ist die weit verbreitete Programmiersprache PHP, auf der ein Großteil des gesamten Internets basiert. Foto: Rob Engelaar/ANP/dpa

Gesamte IT-Branche unter Zeitdruck

Unter dem Namen „PHP2Shell“ warnen Sicherheitsexperten vor gleich zwei kritischen Schwachstellen im Kern der Programmiersprache, die unter den offiziellen Registriernummern CVE-2026-109618 und CVE-2026-109619 geführt werden. Das Gefahrenpotenzial dieser Lücken ist demnach extrem hoch: Kriminelle Akteure können die Schwachstelle ausnutzen, um aus der Ferne eigenen Schadcode auf den betroffenen Servern auszuführen.

In der Praxis ermöglicht dies Angreifern, die vollständige Kontrolle über eine Website zu übernehmen, sensible Kundendaten abzugreifen oder die Infrastruktur für weitere Cyberattacken zu missbrauchen.

Da detaillierte Informationen zur Schwachstelle unbeabsichtigt vorab an die Öffentlichkeit gelangten, steht die gesamte globale IT-Branche unter erheblichem Zeitdruck. Branchenexperten befürchten, dass

Kriminelle bereits in Kürze automatisierte Skripte einsetzen werden, um im großen Stil ungeschützte Server im Internet aufzuspiüren und anzugreifen.

Die akute Bedrohungslage zeigt bereits allorts konkrete Auswirkungen im öffentlichen Leben. In Europa haben zahlreiche Kommunen, Behörden, Universitäten und Krankenhäuser auf die Warnungen der Sicherheitsbehörden reagiert und ihre Online-Angebote kurzfristig vom Netz genommen, um möglichen Angriffen zuvorzukommen. So offensichtlich auch in Luxemburg.

Verhaltensregeln für Seitenbetreiber und Nutzer

Für Betreiber von Webseiten, Onlineshops und digitalen Unternehmensplattformen gilt derzeit höchste Alarmbereitschaft. IT-Experten raten dringend dazu, sich unverzüglich mit den zuständigen Systemadministratoren, IT-Dienstleistern oder Webhosting-Anbietern in Verbindung zu setzen. Be-

reitgestellte Sicherheitsupdates für die PHP-Umgebung sowie für genutzte Systeme müssten ohne jeden Verzug eingespielt werden.

Für normale Internetnutzer besteht beim alltäglichen Surfen auf dem Smartphone oder PC zwar kein direkter Handlungsbedarf, da sich die Sicherheitslücke nicht auf den Endgeräten der Anwender befindet, sondern auf den Servern im Hintergrund. Dennoch können Verbraucher indirekt betroffen sein – etwa durch vorübergehende Ausfälle von Onlinediensten oder potenzielle Datenabflüsse auf nicht rechtzeitig geschützten Webseiten.

Die Entwickler der Programmiersprache sowie Hosting-Anbieter weltweit arbeiten derzeit rund um die Uhr daran, korrigierte Softwareversionen bereitzustellen und zu verteilen. IT-Sicherheitsfachleute betonen nachdrücklich, dass es sich bei diesem Vorfall ausdrücklich nicht um Routineupdates handelt, sondern um eine der gravierendsten Sicherheitslagen der vergangenen Jahre.