PHP-Sicherheitsupdate für BENS G5 5.0.x

Sicherheitsupdate – CVE-2026-109618 und CVE-2026-109619

Dieses Update behebt Sicherheitslücken in PHP 8.2, das von BENS G5 5.0.x verwendet wird. Bitte führen Sie die folgenden Schritte aus, um die aktuellen sicherheitskorrigierten PHP-8.2-Pakete auf Ihrem BENS G5-System zu installieren.

Upgrade-Anleitung

1. Laden Sie das BENS G5 PHP-Sicherheitsupdate herunter: **upgrade_5.0.14.bin**
2. Öffnen Sie die **BENS G5-Weboberfläche** und klicken Sie auf das Symbol **„Upgrade“**.
3. Wählen Sie unter **„Step 1: Select and upload file“** das heruntergeladene Upgrade-Paket aus und laden Sie es auf BENS G5 hoch.
4. BENS G5 überprüft das hochgeladene Paket automatisch und informiert Sie darüber, ob ein Neustart des Systems erforderlich ist. In den meisten Fällen ist kein Neustart notwendig.
5. Klicken Sie auf **„Upgrade“**, um die Installation zu starten.
6. Sobald die Meldung **„Step 3: Upgrade successful“** erscheint, wurde das PHP-Sicherheitsupdate erfolgreich installiert.

BENS G5 führt alle erforderlichen Neustarts der betroffenen Dienste automatisch im Hintergrund durch. Ein manueller Neustart dieser Dienste ist nicht erforderlich.

Technische Informationen (Produkt-Errata)

Security Advisory: RLSA-2026:87073
Betroffenes Produkt: BENS G5.0.x
Betriebssystem: Rocky Linux 8
Komponente: PHP 8.2
Update-Typ: Sicherheitsupdate

Beschreibung

Dieses Update behebt Sicherheitslücken in PHP 8.2 und enthält die entsprechenden Sicherheitskorrekturen.

Behobene Sicherheitslücken:

- **CVE-2026-109618:** Ein Fehler bei der Behandlung von Speichermangel während der Verarbeitung von HTTP-Anfragen kann zu Speicherbeschädigungen und zur Ausführung von Schadcode aus der Ferne (Remote Code Execution, RCE) führen.
- **CVE-2026-109619:** Eine fehlerhafte Behandlung schwerwiegender PHP-Fehler kann dazu führen, dass veraltete Anfragezustände erhalten bleiben und eine Use-after-free-Sicherheitslücke entsteht.
- **CVE-2026-91765:** Eine unbegrenzte Rekursion im SOAP-Parser kann zu einer Dienstverweigerung (Denial of Service, DoS) führen.

Referenzen

- Red Hat Security Advisory RHSA-2026:87073
- CVE-2026-109618
- CVE-2026-109619
- CVE-2026-91765

Die Informationen zu den Sicherheitslücken basieren auf dem Red Hat Security Advisory und wurden unter der Lizenz CC BY 4.0 mit Anpassungen übernommen.