

PHP-Sicherheitsupdate für BENS G5 PP 5.0.x

Sicherheitsupdate – PHP 7.4

Dieses Update behebt mehrere Sicherheitslücken in PHP 7.4, das von BENS G5 PP 5.0.x verwendet wird, darunter CVE-2026-109618 und CVE-2026-109619. Bitte führen Sie die folgenden Schritte aus, um die aktuellen sicherheitskorrigierten PHP-7.4-Pakete auf Ihrem BENS G5 PP-System zu installieren.

Upgrade-Anleitung

1. Laden Sie das BENS G5 PHP-Sicherheitsupdate herunter: **upgrade_5.0.14-php74.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 startet alle betroffenen Dienste automatisch im Hintergrund neu. Ein manueller Neustart der Dienste ist nicht erforderlich.

Technische Informationen (Produkt-Errata)

Security Advisory: RLSA-2026:87080

Betroffenes Produkt: BENS G5 PP 5.0.x mit PHP 7.4

Betriebssystem: Rocky Linux 8

Komponente: PHP 7.4

Update-Typ: Wichtiges Sicherheitsupdate

Beschreibung

Dieses Update behebt mehrere Sicherheitslücken in PHP 7.4 und enthält die entsprechenden Sicherheitskorrekturen.

Behobene Sicherheitslücken

- **CVE-2026-93682:** Speicherzugriff außerhalb des zulässigen Bereichs (Out-of-bounds Read) durch einen leeren Location-Header bei HTTP-Weiterleitungen.
- **CVE-2026-6103:** Manipulation von Archiveinträgen durch einen Ganzzahlüberlauf (Integer Overflow) im TAR-Parser.
- **CVE-2025-14181:** Dienstverweigerung (Denial of Service, DoS) durch einen Heap-Pufferüberlauf im SOAP-Client.
- **CVE-2026-91765:** Dienstverweigerung (DoS) durch unbegrenzte Rekursion im SOAP-Parser.
- **CVE-2026-91766:** Mögliche Offenlegung von Zugangsdaten durch domainübergreifende HTTP-Weiterleitungen.
- **CVE-2026-91767:** Offenlegung von Informationen durch ein speziell präpariertes TLS-Serverzertifikat.
- **CVE-2025-1218:** Dienstverweigerung (DoS) durch einen Speicherzugriff außerhalb des zulässigen Bereichs im mysqlnd-Protokollparser.
- **CVE-2026-91768:** Umgehung von Zugriffsbeschränkungen durch einen unvollständigen Vergleich von IPv6-Adressen.
- **CVE-2026-92842:** Offenlegung von Informationen durch einen Speicherzugriff außerhalb des zulässigen Bereichs in Stream-Filtern.
- **CVE-2026-91769:** Mögliche Vortäuschung einer Serveridentität durch den Rückgriff auf den Common Name (CN) bei der TLS-Zertifikatsprüfung.
- **CVE-2026-109618:** Eine fehlerhafte 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.

Weitere Informationen zu den Sicherheitslücken, einschließlich Schweregrad, CVSS-Bewertungen und technischen Details, finden Sie im offiziellen Security Advisory sowie in den nachfolgenden CVE-Referenzen.

Referenzen

- [Red Hat Security Advisory RHSA-2026:87080](#)
- [CVE-2025-1218](#)
- [CVE-2025-14181](#)