PHP Security Upgrade for BENS G5 PP 5.0.x

Security Update – PHP 7.4

This update addresses multiple security vulnerabilities in PHP 7.4 used by BENS G5 5.0.x, including CVE-2026-109618 and CVE-2026-109619. Please follow the instructions below to install the latest security-patched PHP 7.4 packages on your BENS G5 system.

Upgrade Instructions

1. Download the BENS G5 PHP security upgrade package: **upgrade_5.0.14-php74.bin**
2. Open the **BENS G5 Web Interface** and click the **Upgrade** icon.
3. Under **Step 1: Select and upload file**, select the downloaded upgrade package and upload it to BENS G5.
4. BENS G5 will automatically verify the uploaded package and indicate whether a system restart is required. In most cases, no restart is necessary.
5. Click **Upgrade** to start the installation.
6. Once the message **"Step 3: Upgrade successful"** appears, the PHP security update has been successfully installed.

BENS G5 automatically restarts all affected services in the background. No manual service restart is required.

Technical Information (Product Errata)

Security Advisory: RLSA-2026:87080
Affected Product: BENS G5.0.x with PHP 7.4
Operating System: Rocky Linux 8
Component: PHP 7.4
Update Type: Important Security Update

Description

This update addresses multiple security vulnerabilities affecting PHP 7.4 and includes the corresponding security fixes.

Security Fixes

- **CVE-2026-93682:** Out-of-bounds read caused by an empty HTTP redirect Location header.
- **CVE-2026-6103:** Archive entry injection caused by an integer overflow in the TAR parser.
- **CVE-2025-14181:** Denial of service (DoS) caused by a heap buffer overflow in the SOAP client.
- **CVE-2026-91765:** Denial of service (DoS) caused by unbounded recursion in the SOAP parser.
- **CVE-2026-91766:** Potential credential disclosure through cross-origin HTTP redirects.
- **CVE-2026-91767:** Information disclosure through a specially crafted TLS server certificate.
- **CVE-2025-1218:** Denial of service (DoS) caused by an out-of-bounds read in the mysqlnd wire protocol parser.
- **CVE-2026-91768:** Access control bypass caused by incomplete IPv6 address comparison.
- **CVE-2026-92842:** Information disclosure caused by an out-of-bounds read in stream filters.
- **CVE-2026-91769:** Potential server impersonation through Common Name fallback during TLS certificate verification.
- **CVE-2026-109618:** Out-of-memory bailout during request parsing may lead to memory corruption and remote code execution (RCE).
- **CVE-2026-109619:** Improper handling of fatal errors may retain stale request state, resulting in a use-after-free vulnerability.

For additional information, including severity ratings, CVSS scores, and technical details, please refer to the official security advisory and CVE references below.

References

- Red Hat Security Advisory RHSA-2026:87080
- CVE-2025-1218
- CVE-2025-14181
- CVE-2026-109618
- CVE-2026-109619
- CVE-2026-6103
- CVE-2026-91765
- CVE-2026-91766
- CVE-2026-91767
- CVE-2026-91768
- CVE-2026-91769
- CVE-2026-92842
- CVE-2026-93682

Security advisory information adapted from Red Hat, licensed under CC BY 4.0, with modifications.