PHP Security Upgrade for BENS G5 5.0.x

Security Update – CVE-2026-109618 and CVE-2026-109619

This update addresses security vulnerabilities in PHP 8.2 used by BENS G5 5.0.x. Please follow the instructions below to install the latest security-patched PHP 8.2 packages on your BENS G5 system.

Upgrade Instructions

1. Download the BENS G5 PHP security upgrade package: **upgrade_5.0.14.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.

Technical Information (Product Errata)

Security Advisory: RLSA-2026:87073
Affected Product: BENS G5.0.x
Operating System: Rocky Linux 8
Component: PHP 8.2
Update Type: Security Update

Description

This update addresses security vulnerabilities affecting PHP 8.2 and includes the corresponding security fixes.

Security Fixes:

- **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.
- **CVE-2026-91765:** Unbounded recursion in the SOAP parser may lead to denial of service (DoS).

References

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

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