HYOSUNG TNS Technical Bulletin

Technical Bulletin #HTB-2026-012: BlueVerse Suite Not Affected by PHP Vulnerabilities

Issued: 2026-10-27

Subject: Impact assessment of the PHP vulnerabilities on the BlueVerse Suite

Dear Valued Customer,

On October 21, 2026, the NSA published a cybersecurity advisory about two critical vulnerabilities in PHP-based systems: CVE-2026-109618 and CVE-2026-109619. Hyosung TNS reviewed the advisory to see whether it affects **BlueVerse Suite**.

Advisory link: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4630238/nsa-advisory-critical-patches-recommended-for-php-vulnerabilities/

Scope

In this bulletin, “BlueVerse Suite” refers to all Hyosung TNS BlueVerse software products, including ATM terminal applications and server solutions for monitoring, management, and marketing. This assessment applies to all currently supported versions as delivered by Hyosung TNS. It does not cover third-party software or any services that you have installed separately on the same terminals or servers.

Assessment Result

The BlueVerse Suite is NOT affected by CVE-2026-109618 and CVE-2026-109619. No BlueVerse Suite product uses PHP in its application logic, and no PHP runtime is required or used to run them.

Action required: None.

Recommended Housekeeping for Specific Products

The installation packages for the following products include unused PHP sample files. These files are not run by the application, so they do not expose your system to the vulnerabilities above.

- MoniManager V1
- BlueVerseCRM

As a best practice, we recommend removing these files from production servers to keep your environment clean and prevent false positives in security scans. For removal instructions, please use this link: https://hyosung-tns.atlassian.net/wiki/spaces/HQTS/pages/2659025019/How+to+remove+unused+PHP+files

If you have any questions, please contact your Hyosung TNS support representative.

Sincerely,

Hyosung TNS Technical Support