Date: November 2026

Subject: VaultStream™ Server Software Security Advisory – PHP and Brotli Vulnerabilities

Product: VaultStream™ Server Software

Affected Version Models: Versions 10.4, 10.6, and 10.7

Version Models Under Assessment: Versions 10.2.x and earlier

Olympus is committed to supporting the security of our products and customers in maintaining the integrity of their network environments. Medical device manufacturers and health care delivery organizations alike have a shared responsibility to work collaboratively to maintain robust cybersecurity protections.

Following recent public disclosures and increased attention surrounding the PHP vulnerabilities commonly referred to as "PHP2Shell," Olympus has evaluated their impact on VaultStream™ Server Software Versions 10.4, 10.6 and 10.7. Our assessment also addresses the recently disclosed Brotli vulnerability commonly referred to as "Brotli2Shell."

This advisory outlines the vulnerabilities affecting VaultStream™ Server Software Versions 10.4, 10.6 and 10.7, the available security update, and recommended measures to help protect customer environments. Olympus remains committed to supporting customers as we work together to address these vulnerabilities and maintain the security of their systems.

Please note that Version 11.x VaultStream™ Server software is not affected by these vulnerabilities.

While these vulnerabilities have been exploited in other environments, Olympus is not aware of any exploitation of these vulnerabilities in the VaultStream™ Server software at this time. Under certain network access conditions, exploitation could result in unauthorized access to patient information.

Affected Products

Products and Affected Model #s	Vulnerability Number	Vulnerability Name
VaultStream™ Server software Versions 10.4, 10.6, and 10.7	CVE-2026-109618	RCE via OOM corruption
	CVE-2026-109619	RCE via stale global state
	CVE-2026-111497	Out-of-Bounds Write in Google Brotli Decoder

Please note that assessment of VaultStream™ server software version 10.2 and earlier versions remain ongoing. The absence of those versions from the affected-products table should not be interpreted as confirmation that they are unaffected. Olympus will provide additional information as its assessment is completed.

CVSS Scoring Information

CVE ID	CVSS Score	Details
CVE-2026-109618	**8.9**	CVSS:4.0/BE*MAV:N/MAC:H/MAT:P/MPR:N/MUI:A/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H
CVE-2026-109619	**8.9**	CVSS:4.0/BE*MAV:N/MAC:H/MAT:P/MPR:N/MUI:A/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H
CVE-2026-111497	**8.9**	CVSS:4.0/BE*MAV:N/MAC:L/MAT:P/MPR:H/MUI:N/MVC:H/MVI:H/MVA:H/MSC:H/MSI:H/MSA:H

*CVSS:4.0/BE: Environment Score based on our product environment

Vulnerability Overview

Vulnerability Name	Description
CVE-2026-109618 **Vulnerability in PHP core allowing remote code execution.**	**Technical Details:** Memory corruption caused by out-of-memory (OOM) bailout conditions leaving partially initialized structures during request parsing. **Potential Impact:** This vulnerability, if exploited, could allow an attacker to execute an arbitrary code unauthenticated and also could result in memory panic resulting in Denial of Service.
CVE-2026-109619 **Vulnerability in PHP core allowing remote code execution.**	**Technical Details:** Use-after-free / stale global state surviving across requests within the same PHP worker process. **Potential Impact:** This vulnerability, if exploited, could allow an attacker to trigger a deterministic remote code execution and can expose memory contents such as session tokens, user credentials or data.
CVE-2026-111497 **Vulnerability in PHP core allowing remote code execution and memory leaks.**	**Technical Details:** A critical out-of-bounds memory write vulnerability by supplying a maliciously crafter Brotli-compressed stream. **Potential Impact:** This vulnerability, if exploited, could allow an attacker to trigger a process crash, leak sensitive process memory, or execute an arbitrary remote code unauthenticated.

Remediations:

As part of our ongoing cybersecurity commitment, we have released an important security recommendation for VaultStream™ Server software versions 10.4, 10.6 and 10.7 to address the recently identified and published vulnerabilities with CVEs:

- CVE-2026-109618 and CVE-2026-109619 (commonly referred as PHP2Shell).
- CVE-2026-111497 (commonly referred as Brotli2Shell).

Applying this update addresses the above identified vulnerabilities and is recommended to reduce the associated cybersecurity risk. We recommend working with your IT team to install PHP patch version 8.2.35 (Windows package 8.2.35-1) at your earliest convenience.

For details on this patch refer to Appendix A at the end of this notification:

Note:

- **VaultStream™ Server software version 10.6.x and 10.7.x-**nothing is required except updating the PHP software.
- **VaultStream™ Server software version 10.4.x-**be aware of the following product limitations:
    - The System Configuration page under Maintenance will not be accessible and returns a "404 - File or directory not found" error.
      This functionality is typically used during initial system configuration and is unlikely to be accessed on an already deployed system. If configuration changes are required, contact local Olympus® technical support.
    - If a user opens a NORMAL procedure in EasyView and then enters Compare mode, a "404 - File or directory not found" error is displayed. If you experience this, contact local Olympus technical support.

Mitigations:

While applying remediation patches are strongly recommended, for customers who cannot immediately apply the recommended update as specified above, Olympus recommends implementing the following interim compensating controls, as appropriate for the customer's network environment, until remediation can be completed:

CVE-2026-109618, CVE-2026-109619 and CVE-2026-111497:

- Implement firewall rules to detect and block malicious HTTP requests.
- Restrict access to application to authorized IP or user only, limiting exposure to external and internal network.

- Set up enhanced monitoring to detect abnormal HTTP traffic patterns, HTTP 500 errors, process crashes and unusual memory exhaustion on the application server.

As these products are not Internet-facing and access to the hospital network would be required, Olympus recommends alongside the remediations and mitigations outlined above that customers continue to follow established cybersecurity best practices and review Olympus's General Hardening Guide located on our Global Product Security Website.

https://www.olympus-global.com/products/productsecurity/globalpolicy/product-hardening.html

Contact Information

If you have any questions regarding this security advisory, including what version of the VaultStream™ Server software you have or any issue you may have with an Olympus® product, please contact your regional Customer Support Center.

Appendix A: Installing PHP 8.2.35 on VaultStream 10.4, 10.6, and 10.7

Scope

These are the instructions to update the version of PHP for VaultStream v10.4 and v10.6 and v10.7 to PHP v8.2.35 (use the 8.2.35-1 package).

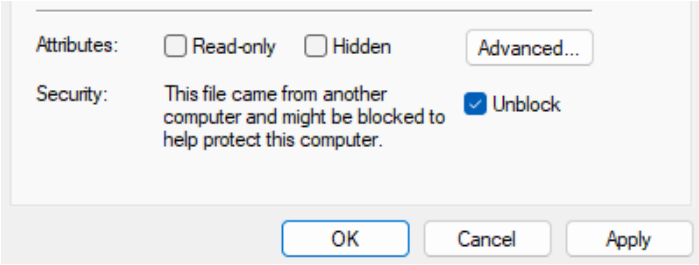
To confirm your VaultStream version

1. Launch a web browser and login to EasyView.
    a. Click the (i) button in the bottom right to view the About Box.
    b. Verify the VaultStream version is 10.4, 10.6, or 10.7



Tools Needed

1. Download **PHP 8.2.35** ***"x64 non-thread safe"*** from https://downloads.php.net/~windows/releases/archives/php-8.2.35-1-nts-Win32-vs16-x64.zip.
2. Right-click the *.zip* file, click Properties, check the "*Unblock*" box and click *OK*.



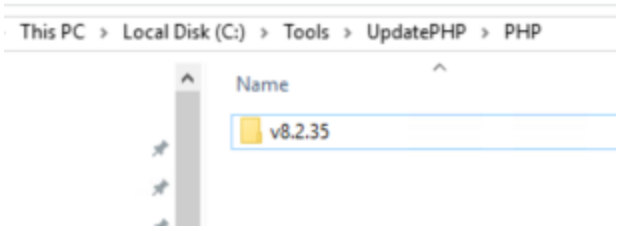
3. Right-click the .zip file, click *Extract All* and then click *Extract*.
4. Rename the extracted folder to **v8.2.35**

Affected Systems

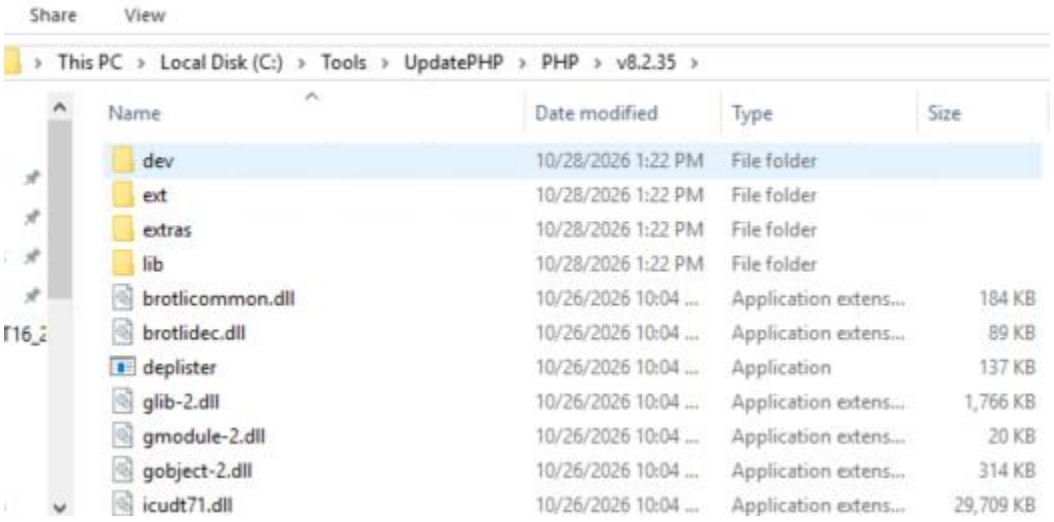
This patch applies to any VaultStream running software version v10.4 and v10.6 and v10.7.

Performing the Update

1) Remote Desktop to the VaultStream and login as an Administrator.
2) Upload the **v8.2.35** folder to the C:\Tools\UpdatePHP\PHP folder

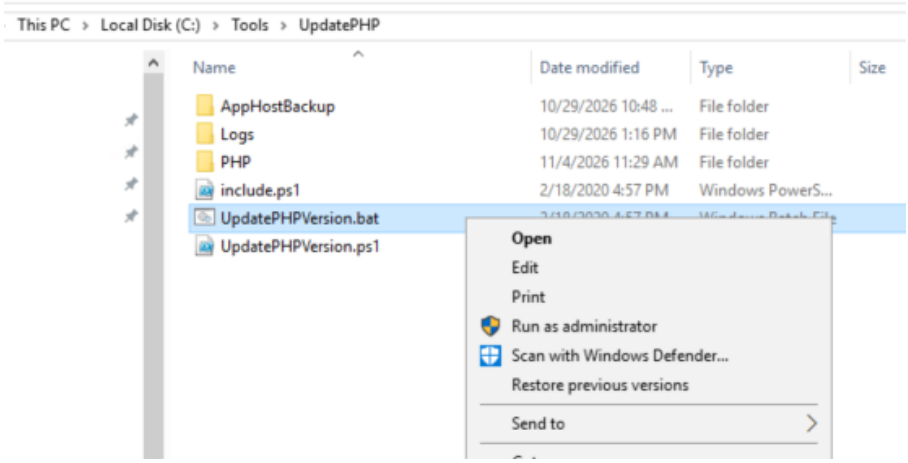


NOTE: the v8.2.35 folder must be in this location C:\Tools\UpdatePHP\PHP folder. See screenshot below:

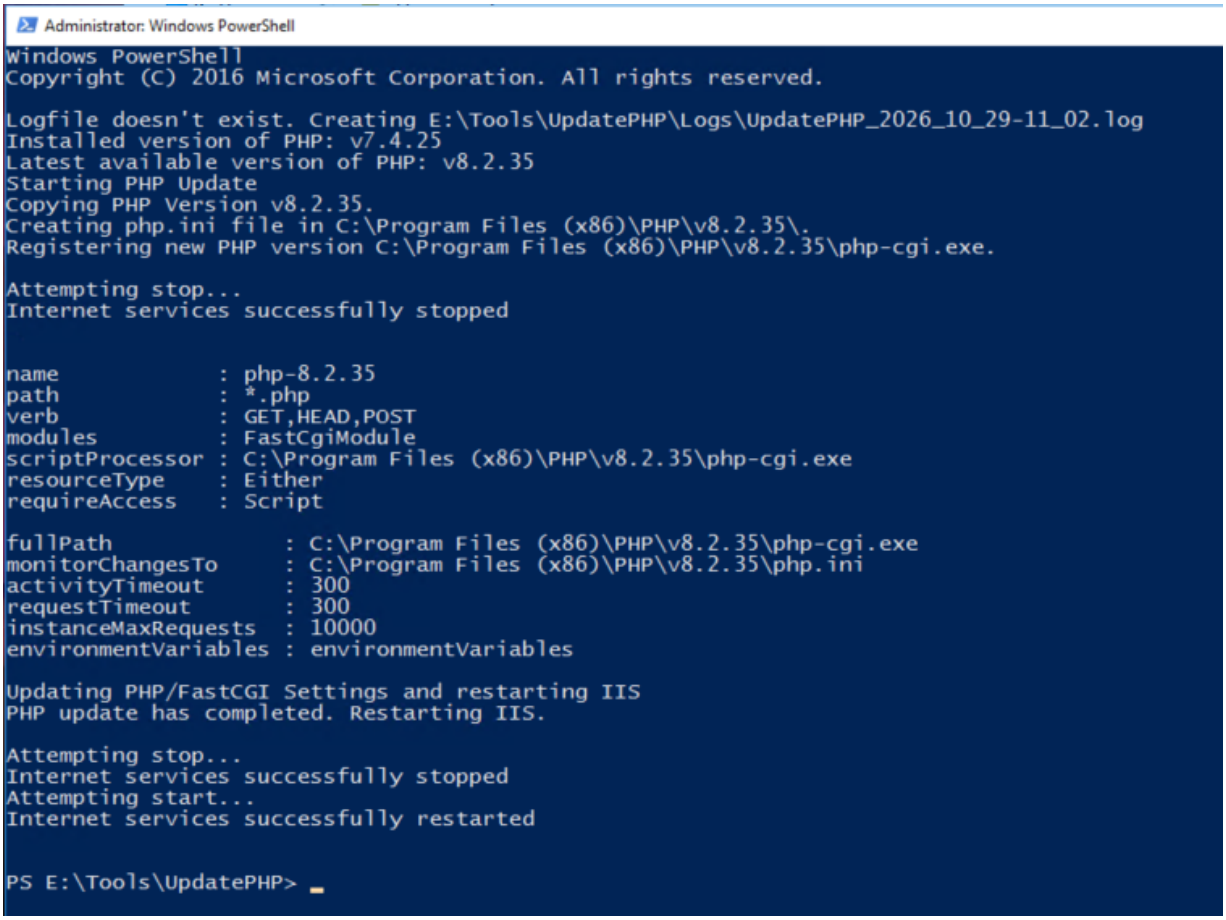


3) Navigate to *C:\Tools\UpdatePHP*.

4) Right-click on *UpdatePHPVersion.bat* and choose "*Run as administrator*" to launch the update tool.



5) A Windows PowerShell window will open and show the progress of the update.



6) The update should take less than a minute.

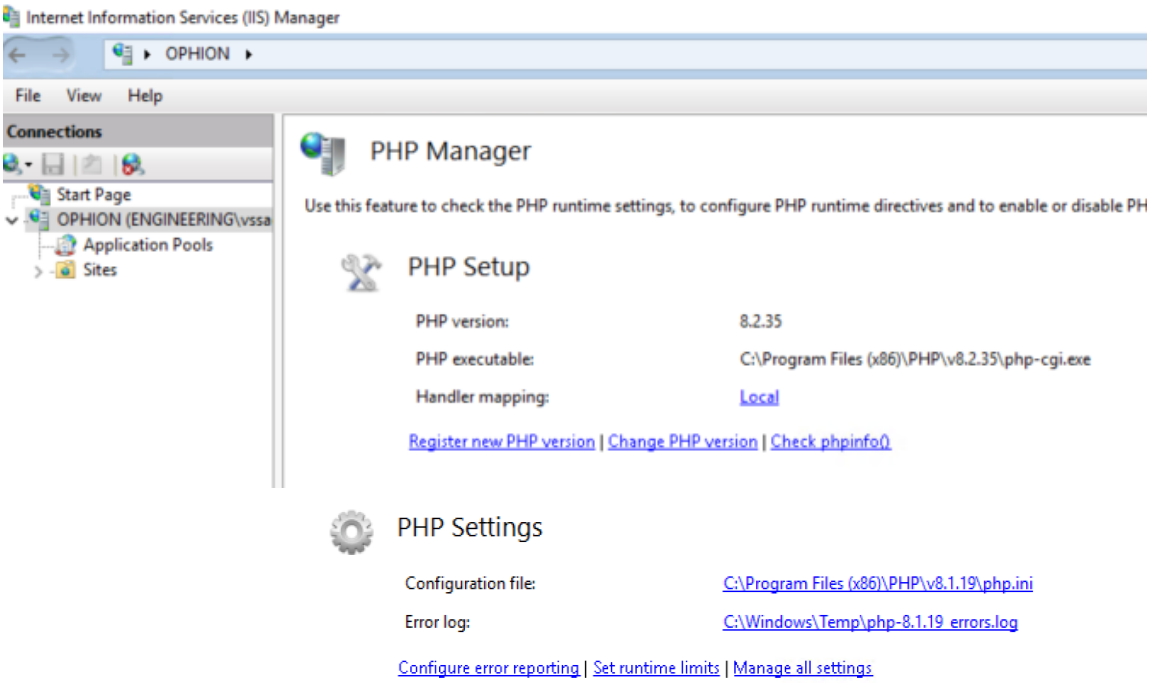
7) Wait for the update to finish.

Validating the Update

1) While still logged in as Administrator, go to the Start menu and select Internet Information Services (IIS).

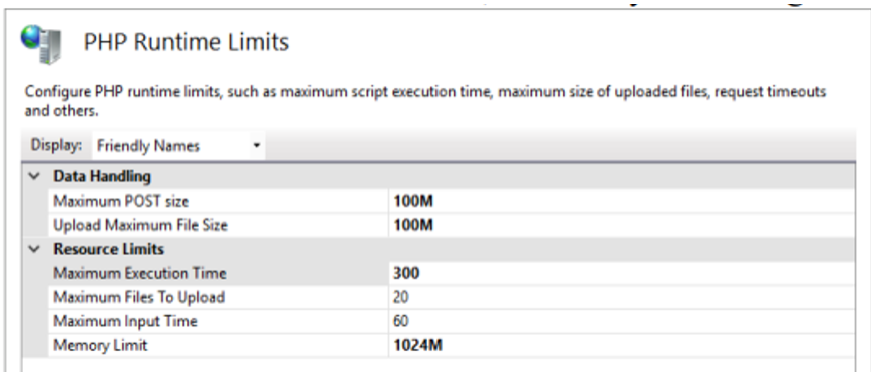
2) In the Internet Information Services (IIS) Manager window, select the system name in the upper left, then in the middle section, in the IIS section, double-click on the PHP Manager.

3) In the PHP Manager, verify that the version of PHP being used in 8.2.35.

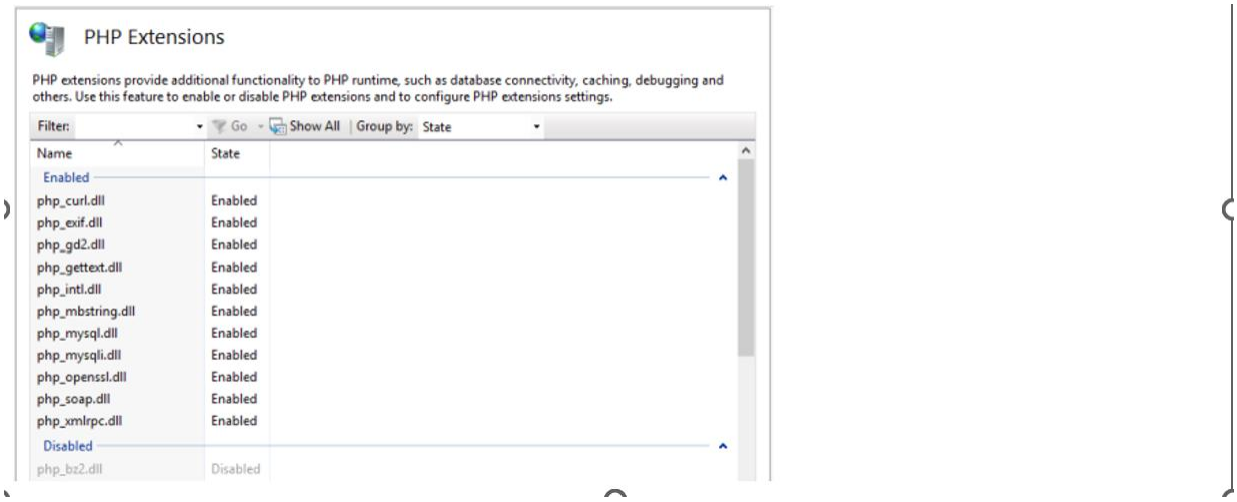


4) Click the Set runtime limits link (depicted at the bottom of the screen above) and verify the settings in the screen shot below are as follows:

- Set Maximum Execution Time to 300
- Set Memory Limit to 1024M

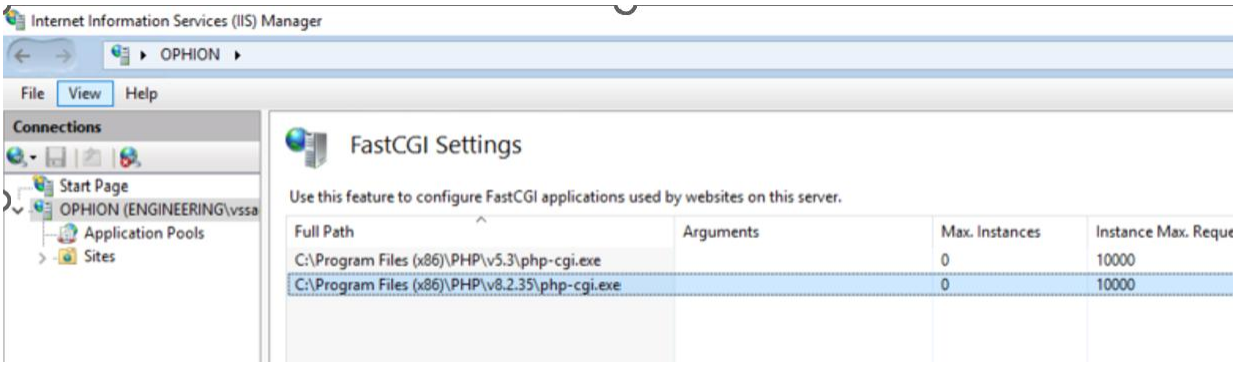


5) Click the Back to main page link on the right, and then select the Enable or disable extensions under the PHP Extensions section. Verify the enabled extensions as shown. If any of the extension in the screen shot show as disabled, set them to enabled:



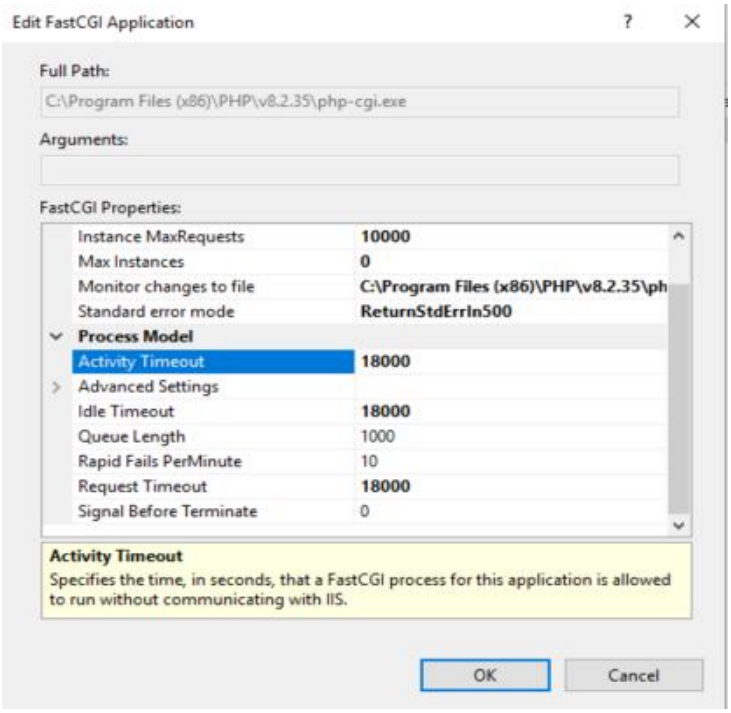
6) Return to the main IIS window. In the middle section, in the IIS section, double-click on the Fast CGI Icon.

7) In the FastCGI Settings windows, verify that 8.2.35 is listed.



8) Double-click on the 8.2.35 listing and verify the Timeout settings as depicted in the screenshot below

- Set "Activity Timeout" to 18000
- Set "Idle Timeout" to 18000
- Set "Request Timeout" to 18000



9) Close the IIS Manager window.
10) Run Command Prompt as Administrator and enter command: *iisreset*
11) Wait until you see message "*Internet services successfully restarted*" then close command prompt window.
12) Launch a web browser and login to EasyView.
13) Click the (i) button in the bottom right to view the About Box.
14) Click the Version Information link in the About Box. Verify the PHP version.