

Jason Eichholz

From: Team Webgility <communication@webgility.com>
Sent: Thursday, October 22, 2026 10:14 AM
To: Jason Eichholz
Subject: Security notice: Critical PHP vulnerabilities on store servers

Hi Jason,

You're receiving this because your online store is, or was, connected to Webgility through our store module, which runs on your store's web server. On October 21, two critical security vulnerabilities were disclosed in PHP, the software that runs that server and many e-commerce platforms. We want to make sure you have what you need to act quickly.

What's happening

- Two critical vulnerabilities (**CVE-2026-109618** and **CVE-2026-109619**, each rated 9.2 out of 10) affect almost every PHP version from 5.4 onward.
- On a server that hasn't been updated, they could let an attacker run code without logging in and could expose passwords or keys the server handles.
- Attempts to exploit them have been reported across the internet since the fix was released.

Is this caused by Webgility?

No. The issue is in PHP itself, at the server level. It affects PHP websites worldwide, whatever apps or integrations they use.

What to do now

1. **Contact your hosting provider or IT team today** and forward them this email.
2. **Ask them to update PHP to a fixed version** (8.5.12, 8.4.27, 8.3.36, 8.2.35 or later) and then restart the web server and PHP services. The fix doesn't take effect until the services restart.
3. **If your server runs PHP 8.1 or older**, those versions no longer receive official updates. Ask about upgrading, or about temporary protection such as a web application firewall.
4. **Once the update is done**, consider changing passwords and keys stored on the server, including your Webgility store module credentials.

More information

- Official PHP website: [php.net](https://www.php.net)
- Official PHP advisory: <https://www.php.net/archive/2026.php#2026-10-21-5>
- Additional guidance from Google Cloud: [Responding to core PHP vulnerabilities](#)

A note on safety: Webgility will never ask for your passwords, payment details or server access by email. If a message claiming to be from us asks for any of these, please contact our support team directly at support@webgility.com.

If you have questions about your Webgility connection, our support team is happy to help at support@webgility.com.

Thank you,
Team Webgility

Webgility, 1111 6th Ave, STE 550, San Diego, CA 92121, USA, (480) 900-0904

[Unsubscribe](#) [Manage preferences](#)