

TrendLife PHP vulnerability web shielding (Web Application Firewall)

Don't let a PHP vulnerability put your website at risk

7-day free service available

Solution Overview:

On October 21, 2026, the [PHP team](#) announced two critical vulnerabilities, CVE-2026-109618 and CVE-2026-109619 (known as PHP2Shell) and released patched versions.

Even a single unpatched PHP vulnerability can lead to service disruption, data loss, or unauthorized access. Both vulnerabilities allow an attacker to run malicious code on the server remotely, without logging in. Each is rated 9.2 (CVSS v4.0), and exploit code was published before the official patch was released.

If you run your own website, check which PHP version it uses and apply all available security updates now. PHP 8.1 and earlier versions may still receive fixes from your hosting provider or Linux distribution, so confirm the patch status with your provider rather than relying on the version number alone. Configuration changes can reduce some risk for a short time, but they do not replace the official security update.

Protection Against **php2shell Attacks**



TrendLife PHP vulnerability web shielding (WAF) adds a protective layer in front of your website to help block PHP2Shell and other web-based attacks before they reach your server. It is a temporary safeguard while you apply the official update and does not replace it.

Helps protect against PHP2Shell and other known PHP exploits. Security rules are optimized for PHP, WordPress, and Laravel websites. Setup is simple with managed protection, and a free SSL certificate is included. Your website continues to work as usual while you patch.

TrendLife is offering a 7-day free service to help everyone get through this tough time. The 7-day free service begins once website protection is activated. To keep protection after the free service, you can subscribe to TrendLife WAF.

TrendLife PHP vulnerability web shielding (WAF) Key Features and Benefits

- **Service Infrastructure:** The service can run on AWS.
- **Multiple Websites Support:** Set up services for multiple websites for your company.
- **Simple Setup:** Get protected in about 20 to 30 minutes. Sign in with your Google account (Google OAuth).
- **7-day free service:** Try the service at no cost before subscribing.
- **Pricing:** After the 7-day free service, you can also purchase through Worry-Free for new or renewal subscriptions. Contact your local service partners (like MSP) for TrendLife Web Proxy or Worry-Free protection.
- **Multiple Services per Account:** Each account can configure and manage multiple services. Each service protects up to 10 hostnames under one main domain.
- **MSP Management Tier:** Accounts on an MSP-managed tier can manage a higher number of services.

Setup Guide: Website Protection (about 20 minutes)

1. Access TrendLife PHP vulnerability web shielding (WAF): Go to <https://waf.trendlife.com> and select Get started.

2. Add Your Website: Give your service a name and enter the website domain visitors use to access your site, such as `www.customer.com`. Each service protects up to 10 hostnames under one main domain.

3. Enter Hosting Details: Enter the server hostname (for example, `origin.example.com`) or the public IP address where your website is currently hosted.

4. Choose a Certificate

Choose one option. The certificate must cover all hostnames associated with this service. We verify this during setup.

- **Automatic Certificate:** TrendLife automatically issues and renews SSL certificates at no additional cost. You need to add a DNS record to verify domain ownership.
- **Use Your Own:** Upload an existing SSL certificate. You are responsible for renewing and replacing it before it expires.

5. Review Your Settings: Check your settings before you activate protection. After the service is created, you cannot edit these settings. To change them, delete the service and create a new one.

6. Activate Protection: Select Activate Protection to start protection. Your 7-day free trial begins once protection is activated.

7. Allow CDN/WAF IPs on the Origin Firewall (Action required)

Work with your network administrator to add the CDN/WAF origin IP ranges provided by TrendLife to the origin firewall allowlist. This allows HTTPS traffic from the CDN/WAF to reach your origin server.

8. Verify Origin Connectivity

Test your website through the TrendLife CDN/WAF to confirm the TLS configuration, origin routing, and website functionality.

Note: Direct access to the origin server remains enabled during this step.

9. Update DNS (Action required)

Work with your network administrator to update your website's DNS records to point to the TrendLife CDN edge. Confirm that traffic is routed through the CDN/WAF.

10. Lock Down the Origin Firewall (Action required)

After DNS cutover and verification are complete, work with your network administrator to remove firewall rules that allow direct access to the origin web service from other sources. Keep only the CDN/WAF origin IP ranges provided by TrendLife, plus any necessary administrative and operational access rules.

Contact & Support:

- Contact TrendLife: Trendlife_Contact@trendmicro.com
- More Information: <https://trendlife.com/en-us>