



Cyber-Allarme PHP: a rischio 285 mila siti e-commerce e portali aziendali su WordPress, Joomla, Drupal

Pubblicato il 26/10/2026

Un'ondata di **vulnerabilità critiche** sta scuotendo l'infrastruttura digitale del Paese. A seguito della recente individuazione di **due gravissime falle** all'interno del linguaggio di programmazione **PHP** — segnalate da OpenAI e monitorate dall'**Agenzia per la Cybersicurezza Nazionale (ACN)** e dal CSIRT Italia — il quadro della sicurezza informatica nazionale delinea uno scenario allarmante.

Il [bollettino d'allerta del CSIRT](#) certifica un pericolo concreto di compromissione per centinaia di migliaia di portali web, spingendo le autorità a raccomandare una misura drastica: **mettere offline i siti qualora non sia possibile applicare tempestivamente le patch di sicurezza**.

Che cos'è PHP e perché è così diffuso

Prima di analizzare i dettagli della crisi, è fondamentale comprendere quale sia il ruolo di **PHP** (*Hypertext Preprocessor*) all'interno del panorama digitale globale.

PHP è uno dei **linguaggi di scripting open source più utilizzati al mondo**, progettato per lo sviluppo di applicazioni web e pagine dinamiche. È la **spina dorsale invisibile della maggioranza dei siti internet**:

- **Piattaforme CMS:** Gestisce l'architettura di sistemi diffusissimi come **WordPress** (che alimenta oltre il 40% del web), Joomla e Drupal.
- **E-commerce e portali aziendali:** Negozi online, banche dati e backend aziendali si poggiano su PHP per gestire contenuti e utenti.

Proprio questa **massiccia diffusione** fa sì che qualsiasi vulnerabilità scovata in PHP si traduca immediatamente in una **minaccia sistemica su scala globale**, esponendo milioni di server a potenziali attacchi.

I dati in Italia: l'81,9% dei servizi monitorati è vulnerabile

Secondo i dati di esposizione aggiornati al 25 ottobre 2026 dal CSIRT Italia, la situazione sul territorio nazionale è critica:

- **Servizi PHP rilevati in Italia:** 741.523
- **Servizi potenzialmente vulnerabili:** **285.149** (pari all'**81,9%** dei servizi per i quali è stato possibile identificare la versione).
- **Istanze aggiornate e protette:** Appena **62.981**.

Di fronte a numeri che evidenziano una superficie d'attacco smisurata, l'ACN ha avviato una campagna straordinaria, inviando notifiche di allerta direttamente ai gestori di **circa 60 mila domini** considerati più esposti.

La minaccia "Php2Shell" e i rischi per i server

Il complesso di falle, ribattezzato **Php2Shell**, apre le porte a scenari di rischio elevatissimi. Sfruttando queste falle, i criminali informatici possono **eseguire codice malevolo da remoto, rubare dati sensibili** o utilizzare le infrastrutture colpite per condurre ulteriori attacchi a catena.

Come sottolineato nel bollettino dell'ACN, lo sfruttamento della vulnerabilità consente l'**esecuzione di codice da remoto** (*Remote Code Execution*) in presenza di specifiche condizioni:

"In particolare, lo sfruttamento richiede che il parametro `session.serialize_handler`, inizialmente configurato su `php_binary` o `php_serialize`, venga modificato dinamicamente a `php` prima dell'avvio della sessione e che la funzionalità di monitoraggio dell'avanzamento degli upload risulti abilitata."

Le contromisure e l'indicazione dell'ACN

L'indicazione prioritaria per gli amministratori di sistema resta l'**aggiornamento immediato** del software alle versioni sicure. Tuttavia, laddove l'applicazione delle patch richieda tempi lunghi o sia impossibile, **il consiglio formale dell'Acn è di disattivare temporaneamente i siti**, isolandoli dalla rete per prevenire intrusioni devastanti.

Link notizia: <https://www.acn.gov.it/portale/w/php2shell-aggiornare-immediatamente-i-sistemi-vulnerabili>