ED
Eugenio Damaso
ESG · Finance · Security · AI

GUIDA · PDF · CHECKLIST

PHP2Shell

Checklist di verifica e risposta per PMI e siti aziendali

26 controlli per capire se i tuoi siti sono esposti a CVE-2026-109618 e CVE-2026-109619, chiudere la falla, escludere una compromissione e documentare le azioni.

Aggiornata al 23 ottobre 2026
Verificata sulle fonti ufficiali

Per chi
Titolari, IT manager, fornitori web

Tempo
30–60 minuti per sito

01 · IL QUADRO

Una falla nel motore, *non nel sito.*

IN SINTESI

- **PHP2Shell** è il nome di due falle critiche di PHP, **CVE-2026-109618** e **CVE-2026-109619**, con punteggio **CVSS v4.0 di 9,2**.
- Permettono di **eseguire codice sul server senza credenziali**, su ogni installazione PHP che serve pagine web.
- Le versioni corrette sono **8.5.12, 8.4.27, 8.3.36 e 8.2.35**: aggiornare è l'unica soluzione completa.
- Gli attacchi sono già in corso, alcuni **anteriori alla patch** del 21 ottobre.
- Aggiornare chiude la falla, ma **non rimuove una compromissione già avvenuta**.

PHP è il linguaggio su cui girano WordPress, Joomla, PrestaShop, Magento e buona parte dei gestionali e dei portali aziendali. PHP2Shell non riguarda un plugin o un tema, ma **il motore stesso**: per questo nessun aggiornamento dell'applicazione, da solo, risolve il problema.

Le due vulnerabilità nascono dalla gestione della memoria. Nella prima, un esaurimento di memoria lascia alcuni dati della richiesta inizializzati solo in parte; nella seconda, PHP conserva riferimenti a memoria già liberata, che una richiesta successiva può sfruttare. In entrambi i casi un attaccante può far eseguire al server **comandi a sua scelta**, il primo passo per installare una *web shell*, cioè una porta di servizio permanente.

Sono coinvolte tutte le modalità con cui PHP serve il web: **PHP-FPM, Apache con mod_php, php-cgi, FrankenPHP e LiteSpeed**. Le configurazioni con mod_php sono considerate le più esposte.

Cronologia essenziale

DATA	EVENTO
17 ottobre 2026	Primo tentativo di sfruttamento rilevato da Amazon, quattro giorni prima della divulgazione
20 ottobre 2026	I dettagli circolano online; il team PHP anticipa un rilascio straordinario
21 ottobre 2026	Escono le versioni corrette; la CISA chiede di aggiornare subito; watchTowr osserva attacchi attivi

Il punto per il vertice aziendale. Il rischio non si chiude con la patch: esiste una finestra, dal 17 ottobre all'aggiornamento, in cui i sistemi potrebbero essere stati raggiunti. Serve una verifica, e serve che sia documentata.

© 2026 Eugenio Damaso · Aggiornata al 23 ottobre 2026

02 · LE VERSIONI

Sei esposto? *Parti dal numero di versione.*

RAMO PHP	VULNERABILE SE	PRIMA VERSIONE SICURA
PHP 8.5	precedente alla 8.5.12	🟢 **8.5.12**
PHP 8.4	precedente alla 8.4.27	🟢 **8.4.27**
PHP 8.3	precedente alla 8.3.36	🟢 **8.3.36**
PHP 8.2	precedente alla 8.2.35	🟢 **8.2.35** · supporto fino al 31/12/2026
PHP 7.4 · 8.0 · 8.1	tutte le versioni	🟡 patch della distribuzione, fornitore LTS o backport ufficiali del codice sorgente
PHP 7.3 e precedenti	tutte le versioni	🔴 nessuna correzione: migrazione

Server dedicato o VPS

Esegui `php -v`, ma verifica anche la versione usata dal web server (PHP-FPM o mod_php), che può essere diversa da quella della riga di comando.

Su Debian, Ubuntu e Red Hat le patch arrivano spesso **senza cambiare il numero principale**: controlla il changelog del pacchetto e cerca i due CVE.

Hosting condiviso o gestito

Crea un file `info.php` con `<?php phpinfo();`, leggi "PHP Version" e **cancellalo subito**.

I pannelli spesso mostrano solo il ramo (es. "8.5"). Se la versione non è corretta, chiedi al provider una **conferma scritta** della patch.

Mitigazioni temporanee, se non puoi aggiornare oggi

Indicate dal team PHP come misure ponte. Non chiudono completamente le falle e non sostituiscono l'aggiornamento.

CVE	MISURA
CVE-2026-109618	`memory_limit=-1` non modificabile dalle applicazioni, `post_max_size` basso, limiti alla dimensione delle richieste su web server o proxy. Da rivedere dopo l'aggiornamento.
CVE-2026-109619	`session.upload_progress.enabled=0` e riavvio di tutti i worker. Su PHP 8.5 anche `fatal_error_backtraces=0`.

> **Cosa non serve.** Disattivare SSH, cambiare le password o aggiornare il CMS sono buone pratiche, ma non chiudono PHP2Shell: l'attacco passa dalle normali richieste HTTP al sito.

© 2026 Eugenio Damaso · Aggiornata al 23 ottobre 2026

03 · LA CHECKLIST

26 controlli, *in cinque aree.*

Spunta ogni voce solo quando hai un'evidenza: uno screenshot, un ticket, una riga di log, un verbale. Una conformità dichiarata e non dimostrabile non regge.

A Inventario

5 controlli

- [ ] A1 **Elenco completo dei siti e delle applicazioni PHP**
  Sito istituzionale, e-commerce, gestionali, portali clienti, intranet, ambienti di test esposti.
- [ ] A2 **Per ognuno: dove gira e chi lo gestisce**
  Server interno, VPS, hosting condiviso, fornitore esterno. Referente e contatto.
- [ ] A3 **Modalità di esecuzione di PHP**
  PHP-FPM, mod_php, php-cgi, FrankenPHP, LiteSpeed. Priorità a mod_php.
- [ ] A4 **Sistemi dimenticati**
  Vecchi siti, landing di campagne, sottodomini, copie di staging ancora online.
- [ ] A5 **Prodotti che includono PHP**
  Appliance, pannelli di gestione e software di terze parti che usano PHP al loro interno.

B Verifica dell'esposizione

5 controlli

- [ ] B1 **Versione completa di PHP rilevata per ogni sistema**
  Non il solo ramo: serve il numero esatto, dal runtime che serve il web.
- [ ] B2 **Confronto con le versioni sicure**
  8.5.12, 8.4.27, 8.3.36, 8.2.35 o patch equivalente documentata.
- [ ] B3 **Changelog dei pacchetti di distribuzione verificato**
  Dove la versione non cambia, cerca i due CVE nel changelog.
- [ ] B4 **Conferma scritta di provider e fornitori**
  Per hosting gestiti e siti affidati a terzi: data e versione della patch.
- [ ] B5 **File di test rimossi**
  Nessun `info.php` o pagina phpinfo lasciata online dopo il controllo.

© 2026 Eugenio Damaso · Aggiornata al 23 ottobre 2026

C Correzione

5 controlli

- [ ] C1 **PHP aggiornato su tutti i sistemi in elenco**
  Ogni runtime, non solo quello principale.
- [ ] C2 **Servizi riavviati**
  Apache, PHP-FPM e ogni worker PHP a lunga esecuzione. Senza riavvio la patch può non essere attiva.
- [ ] C3 **Versione verificata dopo l'aggiornamento**
  Nuovo controllo del numero di versione servito al web.
- [ ] C4 **Mitigazioni temporanee rimosse o riviste**
  In particolare `memory_limit=-1`. Lasciare spento `session.upload_progress` se non serve.
- [ ] C5 **Piano per i rami fuori supporto**
  PHP 8.1 e precedenti: data di migrazione e responsabile. PHP 8.2: migrazione entro il 31/12/2026.

D Verifica di compromissione

6 controlli

- [ ] D1 **File PHP nuovi o modificati dal 17 ottobre**
  Priorità a cartelle di upload, cache, temi e plugin.
- [ ] D2 **Ricerca di codice sospetto**
  `eval`, `base64_decode`, `gzinflate` applicati a input esterni: segnali tipici di web shell.
- [ ] D3 **Integrità del CMS**
  Confronto con i file originali; su WordPress `wp core verify-checksums` o uno scanner come Wordfence.
- [ ] D4 **Analisi dei log**
  Richieste POST anomale o molto grandi; nei log di PHP-FPM errori di memoria o crash ripetuti.
- [ ] D5 **Account e automatismi**
  Utenti amministratori, attività pianificate, chiavi e token creati di recente e non riconosciuti.
- [ ] D6 **Backup completo eseguito e conservato**
  Utile per il ripristino e come prova per ricostruire cosa è successo.

© 2026 Eugenio Damaso · Aggiornata al 23 ottobre 2026

E Governance e NIS2

5 controlli

- [ ] E1 **Responsabile della risposta individuato**
  Una persona che coordina, decide e risponde dei tempi.
- [ ] E2 **Vertice aziendale informato**
  Esposizione, azioni svolte, rischi residui. Per i soggetti NIS2 gli organi di gestione rispondono delle misure.
- [ ] E3 **Valutazione dell'incidente significativo**
  In caso di compromissione, i soggetti NIS2 hanno pre-notifica entro 24 ore e notifica entro 72 ore.
- [ ] E4 **Evidenze richieste ai fornitori ICT**
  Documenti, non rassicurazioni: versione, data dell'intervento, esito delle verifiche.
- [ ] E5 **Registro delle azioni compilato**
  Il modello è nella pagina successiva.

> **Se trovi segni di compromissione:** non limitarti a cancellare i file sospetti. Isola il sistema, conserva log e copie per l'analisi, cambia credenziali e chiavi dopo la bonifica e valuta gli obblighi di notifica.

© 2026 Eugenio Damaso · Aggiornata al 23 ottobre 2026

04 · IL REGISTRO

Documenta ciò che hai fatto, *non ciò che intendi fare.*

Una riga per sistema. È la traccia che serve al board, a un auditor o, per i soggetti NIS2, all'autorità.

SISTEMA	GESTITO DA	VERSIONE PRIMA	VERSIONE DOPO	DATA PATCH	ESITO VERIFICHE · EVIDENZA

Le priorità, in ordine

1. **Aggiorna e riavvia.** Ogni ora con un runtime vulnerabile online è esposizione evitabile.
2. **Verifica la compromissione.** La patch protegge da domani, non da ieri.
3. **Documenta e coinvolgi il vertice.** Un percorso tracciato è una posizione difendibile.
4. **Pianifica la migrazione dei rami fuori supporto.** PHP2Shell non sarà l'ultima falla.

Domande frequenti

Aggiornare WordPress o i plugin risolve PHP2Shell?
No. La falla è nel motore di PHP: va aggiornato il runtime sul server.

Ho un hosting condiviso: cosa devo fare?
Verifica la versione con un phpinfo temporaneo e, se non è corretta, chiedi al provider conferma scritta della patch.

Dopo l'aggiornamento sono al sicuro?
Sei protetto da nuovi attacchi. Resta da escludere una compromissione avvenuta prima della patch.

Fonti

- PHP — note di rilascio 8.5.12 e security advisory, 21 ottobre 2026
- CISA — Critical Vulnerabilities in PHP Require Immediate Patching, 21 ottobre 2026
- watchTowr — PHP Remote Code Execution (PHP2Shell), ottobre 2026
- Unit 42, Palo Alto Networks — Threat Brief CVE-2026-109618 e CVE-2026-109619
- Huntress, Recorded Future, Help Net Security, The Hacker News — analisi e cronologia

© 2026 Eugenio Damaso · Aggiornata al 23 ottobre 2026

ED

Eugenio Damaso
ESG Manager, Planning & Control Manager e CISO

Parliamo di ciò che *deve funzionare.*

Valutare l'esposizione, coordinare i fornitori e documentare le azioni è il lavoro di un CISO. Una call conoscitiva di 30 minuti, senza impegno: capiamo insieme priorità, rischi e il formato di collaborazione più adatto.

Prenota una call | CISO as a Service

Approfondisci

PHP2Shell: la news completa
NIS2 in pratica

Strumenti gratuiti

La NIS2 si applica alla mia azienda?
Autovalutazione NIS2

Contatti

eugenio.damaso01@gmail.com
eugeniodamaso.it
Rende (CS) · Italia · UE

Questa guida ha finalità informative e riflette le informazioni pubbliche disponibili al 23 ottobre 2026. Non sostituisce una valutazione specifica dei sistemi. Le verifiche descritte vanno eseguite solo su sistemi di cui si è responsabili. © 2026 Eugenio Damaso. Tutti i diritti riservati.