
NON APRITE
QUELLA PORTA 80
THE PHP CVE CHAINING MASSACRE
OCTOBER 2026

Paolo Rizzello

Qualche riga su chi vi farà perdere dieci minuti di serenità.



SWA · Excellence Innovation Srl

CEO · Dinamica Tech S.r.l.

CTO · Silenta AI



SECURITY CALLS

«No, tranquilli. Per un’altra call di security un buco in agenda lo trovo.»

PHP2Shell: 2 CVE + 1

Un runtime, tre advisory e una settimana movimentata.

PRODOTTO	CVE	DATA	CVSS	TIPO DI PROBLEMA
PHP	CVE-2026-109618	21/10	**9,2 v4.0**	OOM corruption → RCE
PHP	CVE-2026-109619	21/10	**9,2 v4.0**	Stale global state / UAF → RCE
PHP	CVE-2026-115560	23/10	**8,1 v3.1**	Session upload progress → RCE*

*CVSS 8,1 attribuito da Amazon Linux; le prime due valutazioni sono CVSS 4.0. Scale differenti.

PHP MERDA

… OPPURE NO?

Ottobre nero

Non solo PHP: prodotti diversi, vulnerabilità e incidenti di natura differente.

PRODOTTO	CVE / EVENTO	DATA	CVSS	PROBLEMA
NGINX	CVE-2026-15176	14/10	9,2 v4	Heap buffer overflow
eMudhra CA	8 certificati CA	17/10	—	Chiavi intermedie recuperabili
Plex Media Server	Plex2Shell · 4 CVE	20/10	varia	Catena SSRF → RCE
Node.js / Brotli	CVE-2026-111497	21/10	N.D.	Out-of-bounds write
Oracle Java SE	CVE-2026-91403	21/10	9,1 v3	Trust CA / certificati
OpenSSH	Release 10.6	06/10	—	Hardening e security fixes
Tor	Release 0.4.9.14	07/10	—	Correzioni di sicurezza

Vulnerability Discovery: il collo di bottiglia si sposta

L’intelligenza artificiale accelera il finding. Ma chi verifica, corregge e distribuisce?

DISCOVERY

Ricerca automatizzata

Analisi del codice

Bug hunting e PoC

RICERCA OFFENSIVA

REMEDIATION

Triage e validazione

Root cause e patch

Test e distribuzione

DIFESA & MAINTAINER

LA RICERCA ACCELERA. LA CORREZIONE DEVE TENERE IL PASSO.

Identikit di una CVE

Un identificativo. Una vulnerabilità. Molte informazioni utili per decidere.

PHP SECURITY ADVISORY / CVE RECORD

CVE-2026-109618

CRITICAL

RCE via Out-of-Memory corruption

PUBBLICATA	CNA	CVSS 4.0
21 OTT 2026	PHP	9,2 CRITICAL

VERSIONI COINVOLTE · RAMI SUPPORTATI

8.2 < 8.2.35	8.3 < 8.3.36
8.4 < 8.4.27	8.5 < 8.5.12

VECTOR AV:N AC:H AT:P PR:N UI:N VC:H VI:H VA:H

CWE · TIPO DI DEBOLEZZA

CWE-416 Use After Free

CWE-755 Exceptional Conditions

IMPATTO & RICERCA

RCE · Remote Code Execution

Segnalazioni: Calif, Wiz, OpenAI

Anatomia di PHP2Shell

C, memoria, ownership e condizioni eccezionali.

```
// PSEUDOCODICE DIDATTICO

state = alloc();                    // request 1
worker.global = state;
fatal_error();                      // reset saltato
free_request_memory();

use(worker.global);                 // request 2
```

CWE-416

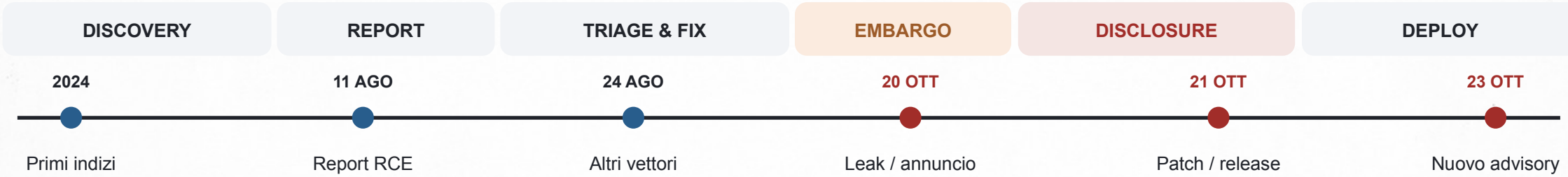
Use-after-free

CWE-755

Error handling

Ciclo di vita di una vulnerabilità

Fasi, embargo e imprevisti: PHP2Shell come caso reale.



DATA	PHP2SHELL: CHE COSA SUCCEDE
2024	Problema OOM ipotizzato; nessun vettore RCE concreto.
11/08	Calif segnala un percorso di RCE; remediation diventa prioritaria.
24/08	Wiz segnala ulteriori vettori; OpenAI contribuisce a nuove analisi.
20/10	ID CVE circolano; Preannuncio e rilascio anticipato di un giorno.
21/10	Embargo infranto; Rilasciate le patch PHP 8.2–8.5.
23/10	Advisory aggiuntivo su session.upload_progress.



CI STANNO HACKERANDO!

STACCA! STACCA! STACCA!

Come reagiamo a una CVE?

Non sempre abbiamo tutti i dettagli. Non sempre abbiamo subito una patch.

01	**RICEZIONE**	Inventario, versione, esposizione: siamo davvero coinvolti?
02	**RISCHIO IMMEDIATO**	Se è inaccettabile: limitiamo l’esposizione, isoliamo o sospendiamo.
03	**IL VETTORE È NOTO**	WAF, configurazioni e disabilitazioni: mitigazioni temporanee.
04	**LA PATCH ARRIVA**	Upgrade o backport supportato, test ed emergency release.
05	**VERIFICHIAMO**	Tutte le istanze corrette? Indicatori di compromissione?

NON IMPATTA? DOCUMENTIAMO. NON POSSIAMO CORREGGERE? RISCHIO RESIDUO, OWNER E SCADENZA.

La sicurezza inizia prima

La capacità di reagire si costruisce quando non c’è un’emergenza.

01 CONOSCERE

Asset, SBOM, versioni e dipendenze realmente in uso.

02 SVILUPPARE

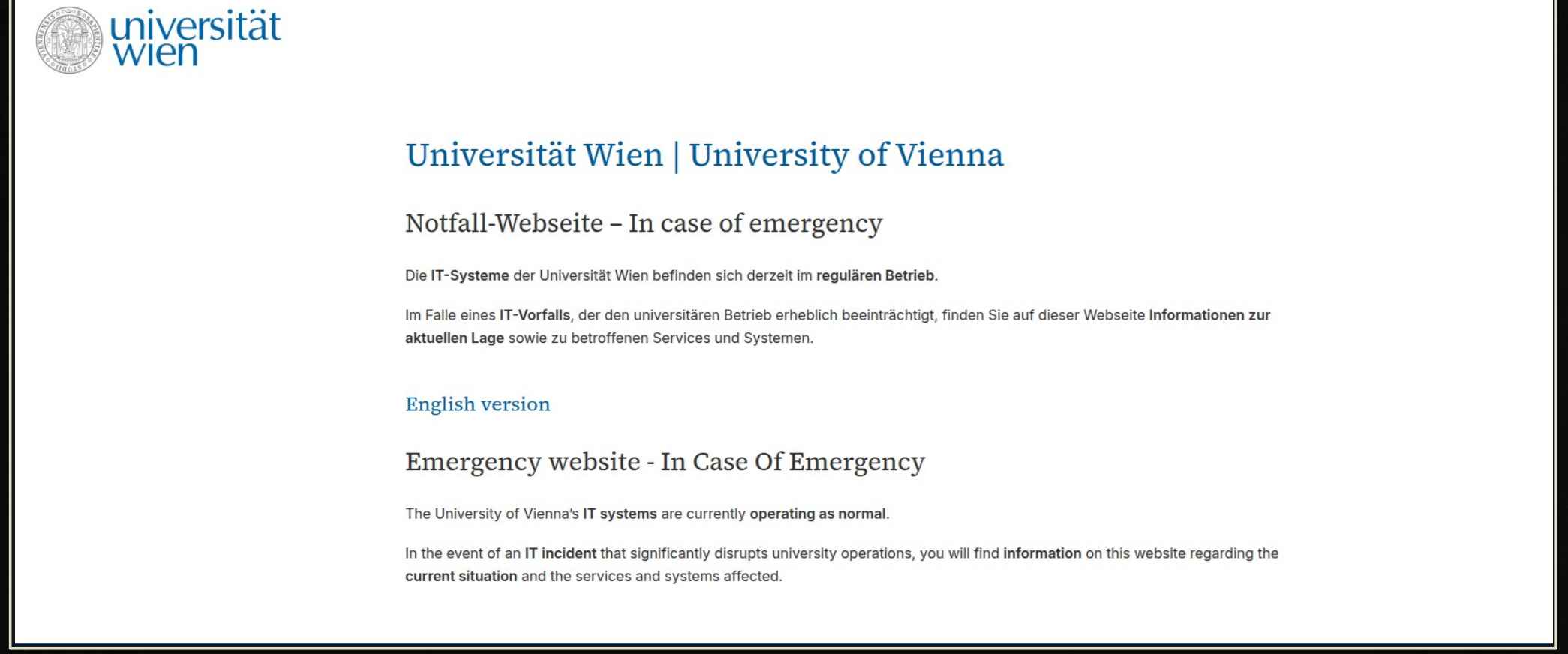
Threat modeling, secure coding e privilegi minimi.

03 VERIFICARE

Code review, SAST, SCA, DAST, test e fuzzing.

04 MANTENERE

EOL, advisory, patch management e pipeline CI/CD.



SE NON C'È LA PATCH...

...NON C'È LA PATCH.

LE ULTIME PAROLE FAMOSE

«Ma chi vuoi che attacchi proprio noi?»

«Abbiamo sempre fatto così.»

«Se funziona, non si tocca.»

«Non possiamo aggiornare: si rompe tutto.»

«Tanto abbiamo il WAF.»

«Lo facciamo alla prossima release.»

NESSUNA DI QUESTE È UNA STRATEGIA DI SICUREZZA.

E quando arriva la prossima CVE?

Cinque domande che distinguono una risposta preparata da un’emergenza infinita.

01 Sappiamo dove gira il componente vulnerabile?

02 Chi valuta il rischio e autorizza l’intervento?

03 Quanto tempo serve per mettere in sicurezza il servizio?

04 Sappiamo distribuire una correzione senza improvvisare?

05 Come dimostriamo di aver eliminato l’esposizione?

SIAMO DAVVERO PREPARATI A REAGIRE AL PROSSIMO BLACK OCTOBER?

LE VULNERABILITÀ SONO INEVITABILI.
L'IMPREPARAZIONE NO.