VEN · 23.10

Pop& Go →

Vendredi LA PLUS CHAUDE

70 % du web à mettre à jour d'urgence

tout ce qu'il faut savoir →



80

Pop & Go

10 SLIDES · À ENREGISTRER

swipe →

LA PLUS CHAUDE

02 · CE QUI S'EST PASSÉ

Deux failles, une fuite, une course

Le 21 octobre, PHP a publié en urgence 4 versions qui corrigent 2 failles critiques.

Elles permettent de lancer du code sur un serveur, sans aucun mot de passe.

Prévue le 22, la sortie a été avancée d'un jour après une fuite sur les réseaux.



premiers indices dès 2024

Source : PHP Foundation · 21/10

suite → 2/10

Trois chiffres pour situer

70 %

des sites du monde tournent sous PHP

Wiz Research · 21/10

9,2

sur 10 : la gravité officielle des failles

PHP Foundation · 21/10

15

failles publiées par PHP depuis le 1er juillet

PHP Foundation · 21/10

la fuite disait 10 sur 10

Source : PHP Foundation · 21/10, Wiz Research · 21/10

LA PLUS CHAUDE

04 · COMMENT ÇA MARCHE

Une attaque en quatre temps

1. Une requête pousse PHP à court de mémoire au mauvais moment.
2. PHP laisse derrière lui des données à moitié prêtes.
3. Une requête suivante réutilise cette mémoire abîmée.
4. L'attaquant y glisse son code et prend la main.

aucun mot de passe requis

Source : PHP Foundation · 21/10

LA PLUS CHAUDE

05 · À FAIRE

Ce que tu peux faire

>_ Tu as un site ? Regarde ta version de PHP dans l'espace de ton hébergeur.

>_ Tu gères ton serveur ? Passe à 8.5.12, 8.4.27, 8.3.36 ou 8.2.35.

>_ Joueur de FF14 ? La sauvegarde côté serveur était encore coupée le 22/10.

le 1, ça prend 2 minutes

Source : PHP Foundation · 21/10, Eurogamer · 22/10

Les zones floues

? Le correctif couvre les versions suivies de PHP, pas les plus anciennes.

? Aucune attaque réussie n'était repérée au moment du correctif ; depuis, on ne sait pas.

? Personne ne sait combien de sites restent à mettre à jour.

PHP 5.4 et après : touchés

Source : PHP Foundation · 21/10

Ce que ça change pour toi

→ Ton blog ou ta boutique sous WordPress ? Le risque est chez ton hébergeur.

→ La faille lit aussi la mémoire du serveur, où passent des mots de passe.

→ L'IA trouve les failles plus vite, pour ceux qui défendent comme pour ceux qui attaquent.

le 3, c'est nouveau

Source : Wiz Research · 21/10, PHP Foundation · 21/10

suite → 7/10

Soulagés, mais fâchés

804 points et 52 fils sur Hacker News

POUR · HACKER NEWS

Une parade de trois lignes, trouvée ici, a protégé mon serveur toute la journée.

CONTRE · HACKER NEWS

Rompre l'embargo six heures avant la sortie, c'est accablant pour Chainguard.

et toi, t'as mis à jour ?

Source : Hacker News · 21/10 (traduit)

LA PLUS CHAUDE

09 · SOURCES

Tout vient de là

PHP Foundation — 21/10
Today's PHP Security Release
thephp.foundation/blog

Wiz Research — 21/10
PHP2Shell: critical RCE in PHP
wiz.io/blog

Eurogamer — 22/10
Games hit by PHP vulnerability outages
eurogamer.net

tout est daté, tout se vérifie

suite → 9/10

VEN · 23.10

Pop& Go→

lundi :

ce que t'as loupé

LUN	MAR	MER	JEU	VEN
IA	**Jeu vidéo**	**Design**	**La + chaude**	**La fun**

Enregistre

tout est dedans, sources comprises

Suis Pop& Go→

@popngo.fr · deux news par jour

Commente

ton avis : on lit tout

Pop & Go