Faille PHP : se couper, dernier levier des utilisateurs

Le 21 octobre 2026, des préfectures, le ministère de l'Économie et Météo-France ont fermé leurs sites pour se protéger de deux failles critiques du langage PHP. Le récit a retenu l'urgence, la fuite des identifiants et la course entre correctif et attaquants. Il a moins retenu l'aveu de la fondation qui entretient PHP : le correctif a tardé faute de décision et de moyens, alors que le défaut était repéré depuis 2024. Le mécanisme est celui que Mancur Olson décrivait en 1965 : un bien dont tout le monde profite et que presque personne ne finance laisse à ses utilisateurs, le jour où il cède, un seul geste possible, se couper eux-mêmes.

Par Alexandre Berge · 31 octobre 2026 · 12 min de lecture · Chronique

Un après-midi de sites en maintenance

À la date du 26 octobre 2026, les faits établis sont les suivants. Le 20 octobre, les identifiants de deux vulnérabilités de PHP circulent sur des forums et les réseaux sociaux avant toute publication, avec une date erronée et un score de gravité surévalué. La PHP Foundation avance alors d'un jour la sortie de ses correctifs. Ils paraissent le 21 octobre, vers 16 h, heure de Paris, pour les versions 8.2 à 8.5 du langage. Les deux failles, CVE-2026-109618 et CVE-2026-109619, permettent d'exécuter du code à distance sur un serveur vulnérable sans s'authentifier (autrement dit, de prendre la main sur la machine qui héberge le site). Leur gravité est cotée 9,2 sur 10.

Dans l'après-midi, les sites de plusieurs préfectures, dont la préfecture de police de Paris, deviennent inaccessibles, comme ceux du ministère de l'Économie, de Météo-France et du quotidien Les Echos, selon franceinfo. Le ministère de l'Intérieur explique, d'après BFMTV, avoir procédé « à la mise en maintenance préventive de l'ensemble de ses sites internet exposés » à la demande de l'ANSSI, l'agence nationale de la sécurité des systèmes d'information. Météo-France diffuse ses informations de sécurité météorologique sur ses comptes, « en attendant le rétablissement de nos outils ». Aux Pays-Bas, plusieurs sites gouvernementaux sont également fermés. Selon franceinfo, l'ANSSI indique que plus de 600 000 serveurs utilisent PHP en France.

L'alerte du CERT-FR, le centre gouvernemental de veille et de réponse aux attaques informatiques, est publiée le même jour et mise à jour le 26 octobre. Elle fait état de

tentatives d'exploitation des deux vulnérabilités et recommande d'isoler les équipements affectés, puis de migrer vers une version maintenue. Les versions 5.x à 8.1 du langage, qui ne sont plus maintenues, restent concernées sans correctif officiel. Une troisième vulnérabilité, CVE-2026-115560, a été publiée le 23 octobre.

Ce que la fondation a reconnu le jour même

Le récit de la journée s'est construit autour de l'urgence technique. Le Monde Informatique titre sur des entreprises « sous pression » et détaille les mesures de contournement. La couverture a aussi relevé la fuite qui a précipité le calendrier. Ils laissent dans l'ombre le texte que la PHP Foundation publie le 21 octobre, en même temps que ses correctifs.

La fondation y retrace l'histoire du défaut. En 2024, lors du premier audit de sécurité externe du langage, réalisé par Quarkslab pour l'OSTIF et financé par l'agence publique allemande Sovereign Tech Agency, un développeur sous contrat de la fondation repère les premiers signes d'un problème de gestion de la mémoire. Une exploitation est envisagée, sans scénario concret. Plusieurs correctifs sont proposés, chacun avec un coût : rupture de compatibilité, risque de déni de service ou modification d'extensions tierces. L'équipe de sécurité décide par consensus. Le travail s'enlise pendant des mois. Le 11 août 2026, une société de sécurité signale une prise de contrôle complète issue de la même cause, et le correctif devient prioritaire.

La fondation conclut en ces termes : « the delay was a structural failure, caused by both the security team's decision process and its lack of resources » (le retard a été un échec structurel, causé à la fois par le processus de décision de l'équipe de sécurité et par son manque de ressources). L'organisation qui gouverne le langage reconnaît donc elle-même la causalité. **Le retard ne tient ni à l'attaquant ni à la fuite, mais à une gouvernance sans arbitre et à une équipe sans moyens.** Elle annonce des décisions à la majorité et une intervention plus précoce de sa direction, et appelle entreprises, hébergeurs et administrations qui utilisent PHP à la financer.

Un bien collectif financé par un petit groupe

Les comptes publiés par la fondation donnent l'échelle du problème. En 2025, elle a reçu 730 534 dollars de 536 organisations et particuliers, un nombre de contributeurs qu'elle juge elle-même « substantially less » (nettement inférieur) à celui de l'année précédente. Ses dépenses, 784 376 dollars, ont dépassé ses recettes d'environ 139 000 dollars. Au 1er janvier 2026, onze développeurs sous contrat travaillaient sur le cœur du langage, à temps plein ou partiel, et signaient environ 42 % des contributions au code. Parmi les quinze financeurs de premier rang que nomme le rapport 2025, une seule entité publique figure, la Sovereign Tech Agency allemande.

D'un côté, plus de 600 000 serveurs en France seulement, des administrations, des médias,

des commerces. De l'autre, un budget annuel inférieur au million de dollars, porté pour l'essentiel par une poignée d'entreprises dont le modèle dépend directement de PHP. Cet écart n'est pas une anomalie morale. Il est la conséquence prévisible de la nature du bien.

> **La logique de l'action collective (Olson, 1965)**
>
> Dans *The Logic of Collective Action*, publié en 1965, l'économiste Mancur Olson renverse une évidence : des individus rationnels qui partagent un intérêt commun ne s'organisent pas spontanément pour le servir. Un bien collectif (un bien dont nul ne peut être exclu une fois qu'il existe) profite à chacun, qu'il ait contribué ou non. Dans un grand groupe, la contribution de chaque membre pèse trop peu pour changer le résultat, et chacun a intérêt à laisser payer les autres.
>
> Olson distingue le **groupe latent**, trop vaste pour s'organiser sans contrainte ou sans *incitation sélective* (un avantage réservé à ceux qui contribuent), du **groupe privilégié**, où un membre au moins tire du bien un avantage suffisant pour le financer seul. Il en tire une conséquence qu'il appelle l'*exploitation du grand par le petit* : le membre qui a le plus à perdre supporte une part disproportionnée de la charge, et le bien reste fourni en deçà de ce que le groupe entier voudrait.

Appliqué à PHP, le cadre décrit la situation avec précision. Les utilisateurs du langage forment un *groupe latent* immense : aucun site, aucune préfecture, aucune entreprise ne voit sa sécurité dépendre de son propre don. Quelques acteurs, éditeurs d'outils de développement, hébergeurs et une agence publique allemande, se comportent en membres d'un *groupe privilégié* et financent la maintenance au niveau que leur intérêt propre justifie. Ce niveau suffit à faire tourner le langage. Il ne suffit pas à arbitrer en quelques semaines un correctif difficile, ce qui suppose des développeurs expérimentés en nombre, une équipe de sécurité dotée et une instance capable de trancher.

Couper ses sites, seul geste disponible

Le second effet du mécanisme se lit le 21 octobre. Une organisation qui dépend d'un composant qu'elle ne finance pas et ne gouverne pas dispose de peu de prises sur lui. Elle ne siège pas dans son équipe de sécurité, ne pèse pas sur ses priorités, n'est pas informée du défaut avant sa publication. Il lui reste à attendre le correctif, l'appliquer, et, entre les deux, se retirer du réseau.

La mise hors ligne préventive n'est pas un excès de prudence, mais le seul levier qui reste à un utilisateur sans voix dans la gouvernance du composant. Son coût, service interrompu et activité suspendue, est supporté par l'utilisateur lui-même. Ce coût ne remonte pas vers la fondation, et il n'entre dans aucun calcul de ce qu'aurait coûté un correctif livré deux ans plus tôt. Le défaut repéré en 2024, grâce à un audit financé par un État étranger, s'est donc soldé en 2026 par une fermeture de sites décidée dans l'urgence par un autre État,

qui n'apparaît pas parmi les principaux financeurs.

Log4Shell, ou le précédent que tout le monde a vu

Le cas d'école est récent et a frappé les mêmes organisations. Le 24 novembre 2021, un ingénieur d'Alibaba Cloud signale à la fondation Apache une vulnérabilité de la bibliothèque Log4j, composant de journalisation présent dans d'innombrables logiciels. Rendue publique le 9 décembre 2021 sous le nom de Log4Shell, elle permet elle aussi l'exécution de code à distance. Le Cyber Safety Review Board, instance d'examen des incidents créée par le gouvernement américain, lui consacre un rapport le 11 juillet 2022.

Ce rapport qualifie Log4j de « endemic vulnerability » (vulnérabilité endémique), appelée à rester dans les systèmes pendant des années. Il souligne surtout les risques propres à une communauté du logiciel libre peu dotée et fondée sur le bénévolat, et appelle les acteurs publics et privés à créer des structures centralisées de financement et d'assistance en sécurité.

La parenté avec PHP tient à la structure. Un composant gratuit, présent partout, entretenu par un petit nombre de personnes, et dont les utilisateurs découvrent la dépendance le jour de la crise. Une différence la renforce : dans le cas de Log4j, la fondation Apache avait corrigé vite, et la difficulté se trouvait chez les utilisateurs. Dans le cas de PHP, la fondation reconnaît que le goulot d'étranglement se trouvait chez elle. Quatre ans après le rapport américain, son appel à des structures centralisées de financement n'a pas empêché un correctif de rester bloqué des mois faute d'arbitre et de moyens.

Le mécanisme sans la marque

Le mécanisme se formule sans PHP. **Une organisation qui repose sur un composant collectif qu'elle ne finance pas et ne gouverne pas transfère sa sécurité à la capacité de décision et aux ressources d'un tiers, et ne conserve, en cas de défaut, que des leviers défensifs dont elle paie seule le coût.** Trois conditions le rendent probable : un composant si répandu que chaque utilisateur se croit couvert par les autres, une maintenance financée par quelques acteurs à la mesure de leur seul intérêt, et une gouvernance du composant où les utilisateurs n'ont ni place ni information.

Ces conditions se retrouvent dans la plupart des systèmes d'information. Un site institutionnel repose sur un gestionnaire de contenu, lui-même écrit dans un langage entretenu par une fondation. Une application métier embarque des dizaines de composants dont personne, dans l'organisation, ne connaît les mainteneurs. Le règlement européen sur la cyberrésilience commence à modifier ce paysage : il impose aux fabricants de produits numériques une diligence raisonnable sur les composants libres qu'ils intègrent et crée un statut d'« intendant de logiciels ouverts » pour les organisations qui soutiennent durablement ces composants. Il ne vise pas, en revanche, l'organisation qui exploite un site pour son propre

compte.

Le signe le plus visible tient dans l'inventaire. Une organisation qui ne connaît ni la liste de ses composants critiques ni le nom de ceux qui les entretiennent ne peut pas savoir si elle appartient au groupe qui paie ou au groupe qui attend.

> **Grille de lecture**
>
> 1. L'organisation dispose-t-elle d'un inventaire de ses composants logiciels critiques, y compris ceux qu'embarquent ses progiciels et ses sites ?
> 2. Pour chacun, sait-elle qui en assure la maintenance, avec quel effectif et quel financement publié ?
> 3. Contribue-t-elle, directement ou par ses fournisseurs, au financement ou à la gouvernance d'au moins un de ces composants ?
> 4. Combien de temps faudrait-il pour isoler, corriger puis rétablir un service exposé si le correctif paraissait un après-midi sans préavis ?
> 5. Qui, dans l'organisation, porte le coût d'une mise hors ligne préventive, et ce coût apparaît-il quelque part ?

Ce que dira la prochaine liste de financeurs

Le 21 octobre, des administrations françaises ont protégé leurs usagers en fermant leurs portes, et ce geste était le bon dans l'urgence. Il dit pourtant l'essentiel du mécanisme : la seule prise que ces organisations avaient sur le composant était de s'en retirer. La fuite et les attaquants ont fixé la date de la crise. La *logique de l'action collective* en avait fixé les conditions, en laissant à un petit groupe le soin de financer ce dont un très grand groupe dépend.

L'hypothèse de cette chronique est que la crise modifiera peu la répartition de la charge, faute d'*incitation sélective* nouvelle. Plusieurs indicateurs permettront de la vérifier d'ici fin 2027. Le premier est le rapport de transparence que la PHP Foundation publiera sur l'exercice 2026, comme elle l'a fait le 27 mai 2026 pour 2025 : le nombre de contributeurs, le montant reçu et la présence d'entités publiques parmi les financeurs de premier rang diront si l'appel du 21 octobre a été entendu. Le second est le 11 décembre 2027, date d'application générale du règlement sur la cyberrésilience, qui rendra opposable aux fabricants la diligence sur les composants libres qu'ils intègrent. Le troisième sera la prochaine faille critique d'un composant de cette nature : si elle conduit encore à fermer des sites publics en attendant un correctif, le 21 octobre aura été une structure plutôt qu'un accident.

Note méthodologique

Les faits reposent sur le billet publié par la PHP Foundation le 21 octobre 2026, son rapport de transparence 2025, l'alerte CERTFR-2026-ALE-014 et la presse de référence (franceinfo, BFMTV, Le Monde Informatique). La causalité entre la gouvernance de l'équipe de sécurité, ses ressources et le retard du correctif est assumée, car elle est reconnue publiquement par la fondation. Le chiffre de 600 000 serveurs est attribué à l'ANSSI d'après franceinfo. L'affirmation selon laquelle aucune administration française ne figure parmi les principaux financeurs se limite aux quinze financeurs de premier rang nommés dans le rapport 2025 de la fondation, consulté le 27 octobre 2026. Le rôle des outils d'analyse automatisée dans la découverte de la chaîne d'attaque n'est pas développé, l'auteur ayant choisi de traiter le financement et la gouvernance du composant. Les faits sont arrêtés au 26 octobre 2026.

Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Documents des organisations et des autorités

The PHP Foundation, « Today's PHP Security Release, and How We're Strengthening PHP Security », 21 octobre 2026. https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/

Elizabeth Barron, The PHP Foundation, « The PHP Foundation Impact and Transparency Report 2025 », 27 mai 2026. https://thephp.foundation/blog/2026/05/27/impact-and-transparency-report-2025/

CERT-FR, « Multiples vulnérabilités dans PHP », alerte CERTFR-2026-ALE-014, 21 octobre 2026, mise à jour le 26 octobre 2026. https://cert.cyber.gouv.fr/alerte/CERTFR-2026-ALE-014/

Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques (règlement sur la cyberrésilience), Journal officiel de l'Union européenne. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R2847

Presse de référence

franceinfo, « Préfectures, médias, impôts… De nombreux sites internet inaccessibles afin de corriger une faille de cybersécurité mondiale », 21 octobre 2026. https://www.franceinfo.fr/internet/securite-sur-internet/prefectures-medias-impots-pourquoi-de-nombreux-sites-internet-sont-inaccessibles-mercredi-apres-midi_8247511.html

BFMTV, « Météo France, les sites de préfectures et de ministères : avec la faille PHP critique, les sites web de nombreux organismes gouvernementaux en maintenance », 21 octobre 2026. https://www.bfmtv.com/tech/cybersecurite/maintenance-en-cours-les-sites-internet-de-nombreuses-prefectures-dont-celle-de-police-de-paris-inaccessibles_AD-202610210677.html

Elgodjam Hanna, Le Monde Informatique, « Deux failles critiques dans PHP : les entreprises sous pression », 22 octobre 2026. https://www.lemondeinformatique.fr/actualites/lire-deux-failles-critiques-dans-php-les-entreprises-sous-pression-100866.html

Cadre théorique

Mancur Olson, The Logic of Collective Action. Public Goods and the Theory of Groups, Cambridge (Massachusetts), Harvard University Press, 1965 (édition révisée de 1971 consultée le 27 octobre 2026). https://archive.org/details/mancur-olson-the-logic-of-collective-action-1971

Parallèle historique

Cyber Safety Review Board, « Review of the December 2021 Log4j Event », 11 juillet 2022. https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf