Scope Cyber

La Lettre Cyber

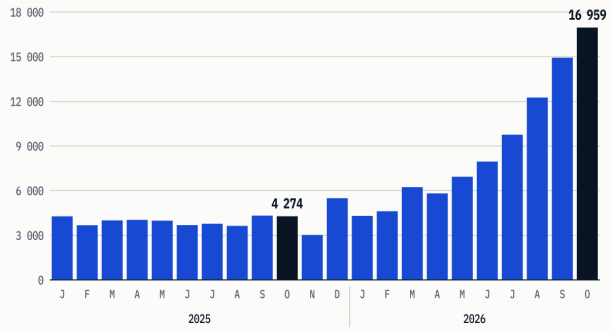
OCTOBRE 2026 · 3 PAGES · SCOPECYBER.FR

LE DOSSIER DU MOIS

Le déluge des failles, accéléré par l'IA

CVE publiées chaque mois

Janvier 2025 – octobre 2026, par mois de publication



De 4 274 CVE en octobre 2025 à 16 959 en octobre 2026. GRAPHIQUE : SCOPE CYBER, DONNÉES CVE TRACKER (CVEPROJECT/CVELISTV5) AU 31 OCTOBRE 2026

Près de 17 000 vulnérabilités ont été publiées en octobre, quatre fois plus qu'un an plus tôt. Une partie vient désormais de systèmes d'IA, qui trouvent les failles et parfois écrivent l'exploit. Les failles réellement exploitées, elles, ne suivent pas la même courbe.

Le volume. Le CVE Tracker suit le référentiel officiel des vulnérabilités. Il a compté 16 959 nouvelles CVE en octobre, contre 4 274 un an plus tôt. Depuis janvier, le total atteint 89 759, presque le double de 2025. Le FIRST, qui fédère les équipes de réponse à incident, en attendait 66 000 sur toute l'année.

Le rôle de l'IA. Le FIRST cite la découverte assistée par l'IA parmi les causes, une « première grande vague ». Il relève aussi des effets de comptabilité : GitHub rattrape d'anciennes failles (+449 % sur un an), VulnCheck en enregistre trente fois plus. VulnCheck reste prudent : le signal est encore émergent. Octobre en donne pourtant deux exemples. Un modèle d'Anthropic a écrit un exploit pour une faille du noyau Linux (ci-dessous). Et la plus grave des failles de Node.js corrigées le 21 octobre a été signalée par OpenAI Codex Security.

Trier plutôt que tout corriger. Le FIRST observe que les failles réellement exploitées n'augmentent pas. Il s'appuie sur deux repères : le catalogue KEV de la CISA, qui recense les failles exploitées, et le score EPSS, qui estime le risque d'exploitation. Les éditeurs doivent s'attendre à doubler leur travail de correction. Pour les systèmes en production, la charge devrait rester stable d'ici fin 2026. « La contrainte n'est plus la découverte », conclut le FIRST : elle tient désormais à la capacité humaine de vérifier et de corriger.

LE CHIFFRE DU MOIS

16 959 CVE publiées en octobre 2026, contre 4 274 un an plus tôt. Le compteur total atteignait 398 637 au 31 octobre.

AU SOMMAIRE

P. 2 VULNÉRABILITÉS ET DONNÉES

PHP2Shell : PHP exploité à distance, avant même l'application

Des certificats émis pour Google après le piratage de registres

Les autres alertes · Données personnelles · Écosystème

P. 3 INCIDENTS ET CONFORMITÉ

Supermarchés : les rayons réfrigérés pris pour cible

Binance : 6,3 milliards de dollars sortis en vingt minutes

Quad9 coupe son DNS sécurisé en France

Réglementation · Chaîne d'approvisionnement

SYSTÈME

Noyau Linux : un exploit distant écrit par une IA



CVE-2026-98432 · CVSS 9,8

Tux, la mascotte du noyau Linux. ILLUSTRATION : LARRY EWING, SIMON BUDIG ET GARRETT LESAGE, VIA WIKIMEDIA COMMONS

La faille CVE-2026-98432, notée 9,8 sur 10, dort dans le noyau depuis Linux 4.4. Un simple paquet SYN portant des options IP la déclenche à l'ouverture d'une connexion TCP. Elle est corrigée en amont et sur les branches stables.

Anthropic, qui l'a signalée, affirme qu'un de ses modèles internes en a tiré un exploit. Celui-ci donne un accès root à distance, sans identifiants, sur les serveurs dotés d'un écouteur Multipath TCP. Il n'est pas publié, et aucune attaque n'est signalée.

Au 30 octobre, Red Hat n'avait pas encore livré de noyau corrigé. AlmaLinux conseille d'ici là de désactiver MPTCP et de filtrer les paquets TCP porteurs d'options IP.

LES INCIDENTS DU MOIS

Supermarchés — Des contrôleurs de réfrigération détournés dans plusieurs enseignes. Page 3.

Binance — 6,3 milliards de dollars sortis en une vingtaine de minutes. Page 3.

Ledger — Un appareil piégé vendu par un revendeur. Page 3.

Infogreffe, LDLC, Quick — Trois incidents confirmés en France. Page 3.

VULNÉRABILITÉS

PHP2Shell : PHP exploité à distance, avant même l'application

Deux failles critiques de PHP ont fuité la veille de leur correctif, puis ont été exploitées. Aucun réglage ne les neutralise : seule la mise à jour protège.

CVE-2026-109618 · CVE-2026-109619

PHP fait tourner une large part des sites web. LOGO : COLIN VIEBROCK, DOMAINE PUBLIC, VIA WIKIMEDIA COMMONS

Le 20 octobre, un outil d'exploitation baptisé « PHP2Shell » a circulé avant l'annonce prévue. PHP a publié le lendemain les versions 8.2.35, 8.3.36, 8.4.27 et 8.5.12. Elles corrigent deux failles qui permettent d'exécuter du code à distance, sans authentification. « La mise à jour est le seul choix sûr », prévient l'équipe de PHP.

Le risque tient à PHP lui-même, quelle que soit l'application. Toutes les installations web sont touchées, mod_php en tête : l'attaque y aboutit avant tout code applicatif. Selon watchTowr, l'exploitation a commencé dès le 21 octobre. Le CERT-FR constate lui aussi des tentatives. Les branches 7.4 à 8.1, en fin de vie, n'ont pas de correctif officiel.

Que faire ? Conserver les journaux, mettre à jour, puis redémarrer les processus PHP. Chercher ensuite webshells et comptes inattendus. Isoler d'Internet ce qui ne peut être corrigé tout de suite. Et suivre les mises à jour des produits qui embarquent PHP.

LES AUTRES ALERTES

GitLab — Une expression régulière piégée dans la CI/CD suffit à prendre la main sur une instance auto-hébergée. La faille, notée 10 sur 10, est corrigée depuis le 12 octobre et exploitée selon la CISA.

Ivanti Connect Secure — Exécution de code à distance, exploitée. Le CERT-FR demande d'isoler l'équipement et de tenir ses secrets pour compromis.

Citrix NetScaler — Deux failles exploitées, parfois avant leurs correctifs, selon le CERT-FR.

Node.js — Dix failles corrigées le 21 octobre, dont une dans le décodeur Brotli. Passer en 22.23.4, 24.22.1 ou 26.12.1.

Aussi exploitées — Cisco AsyncOS, Palo Alto PAN-OS, Windows et BeyondTrust, selon le bulletin du CERT-FR.

WEB

Des certificats émis pour Google après le piratage de registres



Du registre de domaines au certificat : le déroulé décrit par Google. SCHÉMA : SCOPE CYBER, D'APRÈS GOOGLE

Trois registres de domaines nationaux ont été compromis : ceux du Ghana (.gh), de la Sierra Leone (.sl) et des Samoa américaines (.as). Les attaquants ont modifié des enregistrements DNS, puis obtenu des certificats HTTPS pour des domaines de Google et d'autres organisations. Google l'a révélé le 6 octobre.

La confiance dans un certificat repose sur toute la chaîne qui atteste du contrôle d'un domaine, registre compris. D'où le conseil de Google : surveiller les journaux Certificate Transparency, où tout certificat émis est publié.

DONNÉES PERSONNELLES

Fnac Darty : 7 millions d'euros — La CNIL a sanctionné le 22 octobre un traceur déposé sans consentement dans l'application du distributeur.

Hôpital Privé de la Loire : 500 000 € — Un attaquant a consulté les données de 727 113 personnes. Les accès externes n'exigeaient ni VPN ni double authentification, selon la CNIL.

Infogreffe, LDLC, Quick — Infogreffe a confirmé un incident le 12 octobre. LDLC et Quick ont signalé des accès non autorisés.

Notifications Apple — Une nouvelle vague d'alertes est partie le 29 octobre vers des personnes ciblées par des logiciels espions. Le CERT-FR conseille de le contacter sans toucher à l'appareil.

ÉCOSYSTÈME

ECSC 2026 — La Team France a fini 10e sur 42 à Bochum (classement).

Annuaire — Six nouveaux acteurs, dont Ariovis, Axenia et StalkPhish.

Agenda — Le 1er décembre, Journée RGPD de la CNIL à Poitiers.

INCIDENTS

Supermarchés : les rayons réfrigérés pris pour cible

Dans la nuit du 11 au 12 octobre, des contrôleurs de réfrigération accessibles depuis Internet ont été détournés dans des magasins de plusieurs enseignes. Le parquet de Paris a ouvert une enquête.



Photo d'illustration, sans lien avec les magasins touchés. PHOTO : BNUMMER, CC BY-SA 4.0, VIA WIKIMEDIA COMMONS

Les attaquants ont déclenché à distance le dégivrage de contrôleurs Danfoss anciens. La température des meubles frigorifiques est montée. Intermarché et Coopérative U ont confirmé des magasins touchés, dont le nombre reste flou : 250 à 350 selon BFMTV, citée par BleepingComputer.

Le CERT-FR a signalé le 12 octobre de nombreuses compromissions de Danfoss AK-SM et AK-SC. Le 16, il a ajouté des superviseurs Copeland et Dixell. Sa consigne : aucune interface d'administration exposée sur Internet, un accès par VPN uniquement, des plages de dégivrage vérifiées. Froid, chauffage, contrôle d'accès : ces équipements relèvent de la sécurité des objets connectés, au même titre que les serveurs.

RAPPORT DGFIP

Le rapport de l'ANSSI sur les fuites de l'été à la DGFiP, publié fin septembre, relève trois faiblesses :

- des identifiants d'agents volés, faute d'authentification forte ;
- des applications sensibles sans cloisonnement ;
- deux vagues d'exfiltration passées inaperçues.

RÉGLEMENTATION

NIS 2 — La loi Résilience, retirée de l'ordre du jour de l'Assemblée le 6 octobre, attendait toujours une nouvelle date fin octobre, selon Next.

CRYPTO

Binance : 6,3 milliards de dollars sortis en vingt minutes

29 OCTOBRE · ENV. 6,3 MD$

Binance, première plateforme d'échange de cryptoactifs visée. LOGO : BXALBER, CC BY-SA 4.0, VIA WIKIMEDIA COMMONS

Le 29 octobre, environ 6,36 milliards de dollars ont quitté les portefeuilles connectés de Binance en une vingtaine de minutes. C'est le plus gros vol de cryptoactifs jamais enregistré. TRM Labs l'attribue au groupe nord-coréen TraderTraitor.

Binance évoque le poste compromis d'un ingénieur DevOps. Pour TRM Labs, c'est toute la chaîne de signature qui a cédé : sur Ethereum, une délégation EIP-7702 a vidé le portefeuille en une transaction. Environ 2,7 milliards ont été gelés par les émetteurs de stablecoins.

CHAÎNE D'APPROVISIONNEMENT

Ledger — Un appareil vendu par CryptoBilis, revendeur d'Asie du Sud-Est, cachait un implant. Il transmettait la phrase de récupération par le réseau mobile, a confirmé Ledger le 10 octobre. Des tiers estiment les pertes à 93 millions de dollars, un chiffre que Ledger ne confirme pas (CoinDesk). Un cas d'école d'attaque de la chaîne d'approvisionnement.

RÉSEAU

Quad9 coupe son DNS sécurisé en France

Le résolveur public 9.9.9.9 cessera de répondre aux utilisateurs français le 24 novembre. Quad9 refuse de bloquer des sites comme le lui impose la justice.

Saisi par beIN, un tribunal français a ordonné le 21 octobre à Quad9 de bloquer certains noms de domaine pour les internautes en France, sous astreinte. Le service refuse. « Pour nous, la résolution DNS récursive est un service neutre et passif », écrit-il. Il a fait appel.

Le 24 novembre, Quad9 retirera à la fois la résolution DNS et le filtrage des domaines malveillants, qu'il offrait aux Français depuis près de neuf ans. Une vingtaine d'autres procédures visent des opérateurs de résolveurs. Postes, routeurs, serveurs : tout équipement réglé sur 9.9.9.9 doit changer de résolveur avant cette date, et retrouver ailleurs le blocage des domaines malveillants.