

Revue d'actualité de l'OSSIR

13 octobre 2026



← Jérémie De Cock
Melchior Courtois →



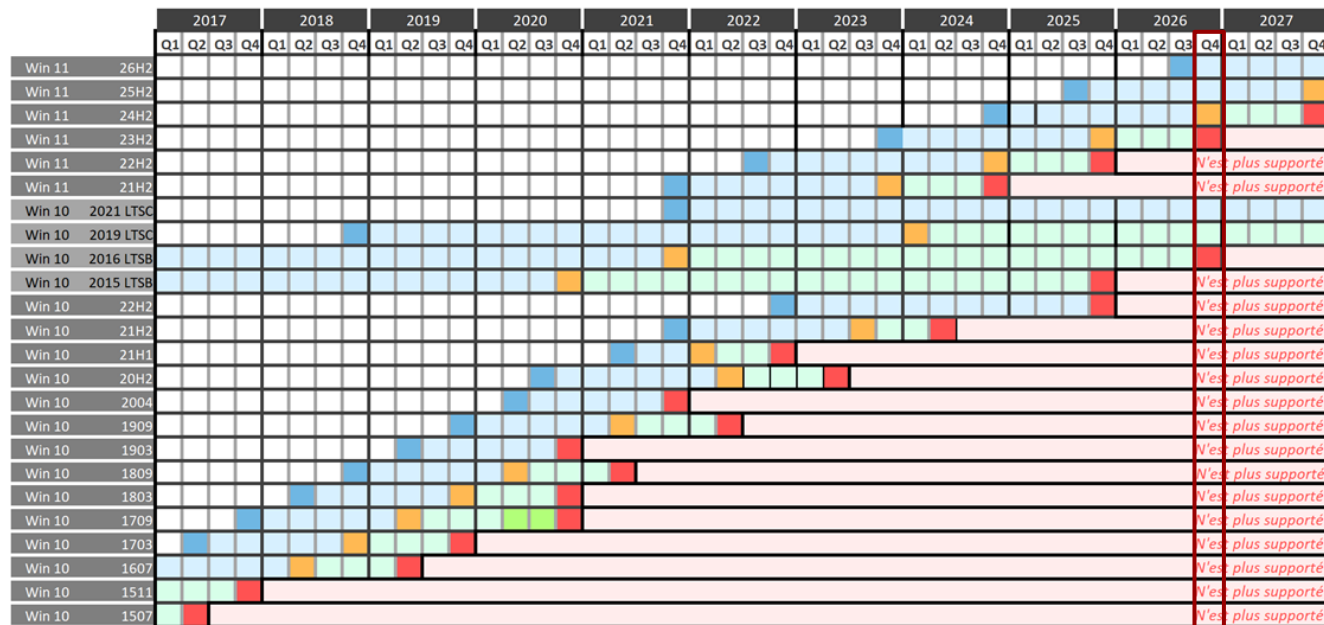
<< La veille vous est fournie par cyberzen >>



Rappel du support Windows en couleurs

Faibles / Bulletins / Advisories (MMSBGA)

Microsoft - Windows Workstation



← Nous sommes là

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSC/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSC/LTSC

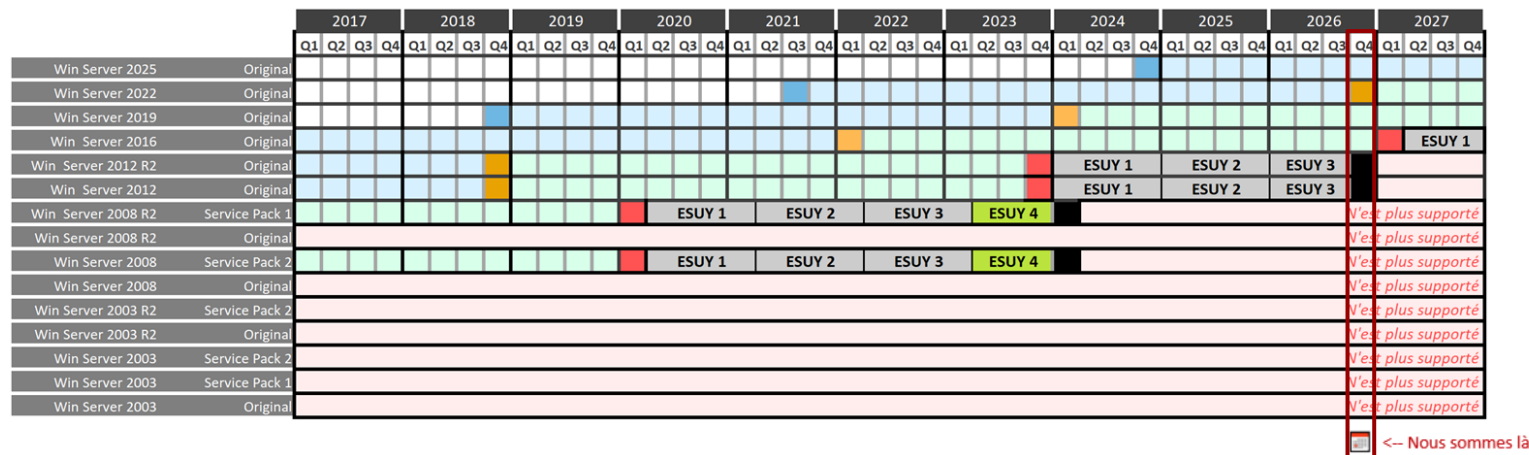
Sortie	Home, Pro	Entreprise
mardi 29 septembre 2026	mardi 10 octobre 2028	mardi 9 octobre 2029
mardi 30 septembre 2025	mardi 12 octobre 2027	mardi 10 octobre 2028
mardi 1 octobre 2024	mardi 13 octobre 2026	mardi 12 octobre 2027
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 18 octobre 2022	mardi 14 octobre 2025	mardi 14 octobre 2025
mardi 16 novembre 2021	mardi 13 juin 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 11 mai 2021
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	9-avril-4 sept. 2019	14-avril-13 oct. 2020
mercredi 5 avril 2017	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	mardi 9 mai 2017	mardi 9 mai 2017

LTSC : Long-Term Servicing Branch
LTSC : Long-Term Servicing Channel



Faibles / Bulletins / Advisories (MMSBGA)

Microsoft - Windows Server



Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024		
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 30 octobre 2012	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 22 février 2011	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
jeudi 22 octobre 2009	mardi 9 avril 2013		
mercredi 29 avril 2009	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
mardi 6 mai 2008	mardi 12 juillet 2011		
mardi 13 mars 2007	mardi 14 juillet 2015		
dimanche 5 mars 2006	mardi 14 avril 2009		
mardi 13 mars 2007	mardi 14 juillet 2015		
mercredi 30 mars 2005	mardi 14 avril 2009		
mercredi 28 mai 2003	mardi 10 avril 2007		

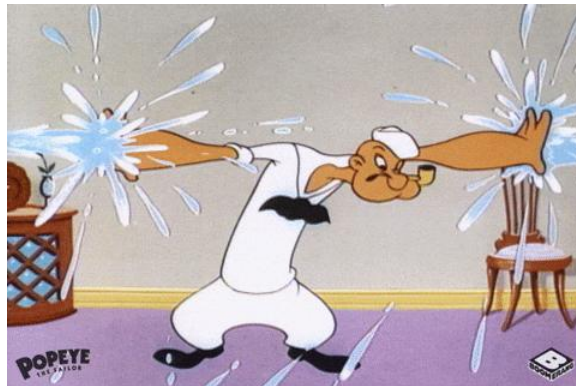
Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour la version standard
- Support étendu pour LTSB/LTSC
- Fin de support étendu pour LTSB/LTSC
- X Extension d'une ou plusieurs années (ESUY)
- X Extension disponible uniquement avec Azure (Microsoft Entra ID)
- Fin de support pour la ou les extensions supplémentaires

ESUY : Extended Security Update Year



Failles / Bulletins / Advisories



■ Patch Tuesday de septembre : 973 failles, un record absolu

- Publié le 8 sept. — 973 CVE dont 113 critiques. Le plus gros de l'histoire, il pulvérise le record de juillet (578 CVE)
 - Windows à lui seul : 723 correctifs (puis Office 111, SQL Server 62)
- 2 zero-day exploitées, 2 élévations de privilèges locales :
 - **[CVE-2026-81963]** Windows Update → SYSTEM (Win 11 / Server 2025)
 - Accès local initial requis sur la machine cible
 - **[CVE-2026-85880]** débordement ALPC, évasion d'AppContainer (Win 10 / Server 2012-2022)
- 20 failles jugées « wormables » (DNS, DHCP, SMB...), dont CVE-2026-69730 à 9,8
- Et le Patch Tuesday d'octobre tombe aujourd'hui même : à compléter en séance

<https://www.it-connect.fr/patch-tuesday-septembre-2026-recapitulatif/>

CVE par Patch Tuesday (2026)

Faibles / Bulletins / Advisories

Microsoft + Navigateur

■ BlueMoon : une chaîne Chrome + Windows 0-day aux mains de plusieurs APT

- Kit chaînant 3 failles, repéré par Volexity/Proofpoint dès le 1er sept.
 - **[CVE-2026-85046]** type confusion V8 + **[CVE-2026-87491]** évvasion sandbox WebAssembly
 - **[CVE-2026-85880]** élévation noyau Windows → sortie de la sandbox Chrome
- « Patch gap » : failles corrigées dans le code Chromium mais pas encore dans le Chrome public → 0-day de fait
- Au moins 4 groupes liés à la Chine (dont APT31) ; cibles : ONG, gouvernements
- La leçon : forcer le redémarrage du navigateur, le cycle de MàJ ne se néglige plus
<https://thehackernews.com/2026/09/chinese-hackers-exploit-chrome-windows.html>



Faibles / Bulletins / Advisories Système

Nightmare Eclipse sort du bois... et continue de harceler Microsoft

- Le chercheur a révélé son identité : Abdelhamid Naceri, ex-employé de Microsoft
- ShieldCrash : 0-day Defender → SYSTEM, publiée juste après le Patch Tuesday
- BigDiskBuster : remplit le disque pile quand Defender se met à jour → l'antivirus reste figé sur de vieilles signatures (déni de service)
 - Fonctionnerait sur toutes les versions de Windows, proche d'UnDefend (avril)
- Et aussi des 0-day visant Kaspersky, Avast, CrowdStrike et NVIDIA
- Près d'une douzaine d'exploits publiés depuis avril, sur fond de conflit personnel

<https://www.it-connect.fr/bigdiskbuster-zero-day-defender-bloque-mises-a-jour/>



■ Exchange : lire la boîte mail de ses collègues avec un simple compte

- **[CVE-2026-96940]** élévation de privilèges, CVSS 8,8 — correctif hors-bande
- Un utilisateur authentifié accède aux boîtes des autres : patron, DSI, compta...
 - Un seul compte phishé/pulvérisé suffit. « Exploitation plus probable » selon MS
- Microsoft publie une V2 des MàJ de septembre : même patché, repasser la maintenance
- Exchange 2016/2019 : plus de correctif sans ESU (support terminé oct. 2025)

<https://www.it-connect.fr/exchange-server-cve-2026-96940/>

Faibles / Bulletins / Advisories

Système / Smartphone

■ Apple : un record de 261 CVE, puis une 0-day CoreGraphics

- 14 sept. — plus grosse salve de l'histoire d'Apple
 - iOS 27 : 122 CVE (dont 20 dans le noyau) · macOS 27 : 204 CVE
 - Volume dopé par l'IA (CVE créditées à Claude/Anthropic et OpenAI Codex)
- 28 sept. — **[CVE-2026-86950]** 0-day CoreGraphics déjà exploitée
 - « Attaque extrêmement sophistiquée contre des individus ciblés », signalée par Meta
 - Un fichier piégé suffit. Corrigée en iOS/iPadOS 26.7.1 et macOS 26.7.1 / 15.8.1

<https://www.theregister.com/security/2026/09/15/the-vulnpocalypse-rains-ibugs-down-on-apple-with-record-setting-number-of-patches/5296679>



Faillles / Bulletins / Advisories

Réseau / Équipements de bordure

La bordure sous le feu : Citrix, Check Point et F5 en une semaine

- Citrix NetScaler — « Éteignez vos NetScaler » : 2 zero-day CVSS 9,5 exploitées
 - **[CVE-2026-88771] + [CVE-2026-88772]**, PoC watchTower, exploitation de masse
- Check Point — **[CVE-2026-85102]** RCE VPN pré-auth exploitée dès le 12 sept. ; + un 0-day du serveur de gestion exploité depuis le 23 juillet
- F5 BIG-IP APM — **[CVE-2026-94127]** CVSS 9,8, RCE non authentifiée (OAuth), déjà exploitée ; plus de 15 000 instances exposées
- Équipement exposé = priorité absolue, scanné dans les heures qui suivent l'avis

<https://www.it-connect.fr/citrix-netscaler-cve-2026-88771-cve-2026-88772-zero-day-exploitees/>



■ Les n-day qu'on a oublié de patcher

- Metabase **[CVE-2026-72898]** : injection SQL non auth → admin
 - Patch du 6 août, exploitation de masse (cf. slide État français)
- Roundcube **[CVE-2026-48842]** : injection SQL pré-auth (plugin virtuser_query), patch de mai, exploitée depuis septembre
- Veeam Agent Windows **[CVE-2026-32996]** : fuite d'UID dans un log → SYSTEM, exploit public (build $\geq$ 13.0.3.1220)
- Dell System Update **[CVE-2026-86360]** : path traversal → root, CVSS 9,6, corrigé en juillet... mais marqué « optionnel »

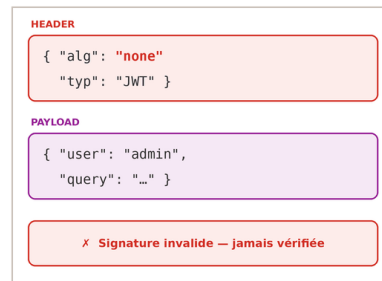
<https://www.it-connect.fr/dell-system-update-faille-critique-cve-2026-86360/>



Microsoft Titan : un jeton JWT non signé ouvre 17 300 milliards de lignes

- Un chercheur de 16 ans accède à Titan, un service d'analyse interne de Microsoft
- L'API vérifiait tenant, audience, app, utilisateur... mais jamais la signature du jeton
 - Il forge un JWT avec l'algorithme « none » et l'utilisateur « admin » → SQL brut
- 17 333 335 124 315 lignes à portée. Corrigé le 9 sept. (prime : 5 000 \$)
- Rappel vieux comme la RFC 8725 : fixer la liste d'algos autorisés, refuser « none »

<https://www.it-connect.fr/microsoft-titan-faible-jwt-sans-signature/>



Microsoft Titan

1 920 Md

Faibles / Bulletins / Advisories

Application / Framework

■ Atlassian : lire des fichiers sur Jira, Confluence et Bitbucket sans s'authentifier

- **[CVE-2026-21589]** path traversal, CVSS 9,3 — 8 produits Data Center
- Lecture de fichiers arbitraires dans la racine web, sans authentification
 - Il faut connaître le chemin — mais les arborescences Atlassian sont standardisées
- PoC watchTowr : via Jira intégré à Crowd → mot de passe en clair → compte admin Jira
- Exploitée depuis la publication du PoC. Patcher + sortir ces instances d'Internet

<https://www.it-connect.fr/atlassian-cve-2026-21589-faible-critique-jira-confluence-bitbucket/>



■ GLPI : la branche 10 tire sa révérence, et l'IA accélère tout

- GLPI 10.0.28 sera la dernière de la branche 10 : plus aucun correctif ensuite
 - GLPI 12 attendu en octobre ; migrer, car l'écart de sécurité se creusera vite
- Rythme des correctifs passé à ~1 fois / 2 semaines (8 failles le 30 sept.)
 - Teclib' l'assume : l'IA découvre les failles plus vite et gonfle le volume
- Même constat chez Microsoft, Apple, Google, Chrome, Ubuntu : le volume explose partout

<https://www.it-connect.fr/glpi-11-0-10-0-28-failles-fin-glpi-10/>

■ Processeurs & hyperviseurs : la fuite ne faiblit pas

- Spectre v2 « BTR » (VUSec) : variante visant les moteurs JIT (cBPF). Vol du hash du mot de passe root sous Linux en 3-5 min, sur Intel, AMD et Arm
 - **[CVE-2026-64507]** / **[CVE-2026-64508]** — atténuation IBPB déjà intégrée au noyau
- KVM : 4e évocation invité → hôte de Hyunwoo Kim cette année (Januscape, ITscape, Zapscape) ; et une évocation revendiquée via Vercel/Firecracker le 6 oct.
 - Un locataire peut atteindre l'hôte et les autres VM d'un cloud mutualisé

<https://www.it-connect.fr/spectre-v2-btr-linux-hash-mot-de-passe-root/>

<https://thehackernews.com/2026/09/new-linux-kernel-flaw-gives-arm64-kvm.html>



SPECTRE

■ Deux coups portés aux fondations : mémoire chiffrée et RSA

- DDRop : un interposer DDR5 à 159 \$ casse l'intégrité du confidential computing
 - Intel TDX/SGX et AMD SEV-SNP : en « droppant » des écritures, le CPU relit d'anciennes données chiffrées (rejeu) — jusqu'au mode debug d'une VM et à la forge d'attestation (accès physique)
- RSA : forger des signatures RSA-1024 sans factoriser la clé (UC San Diego/Inria)
 - Nécessite un oracle de signature brut ; même 4096 bits n'atteindrait plus 128 bits dans ce modèle → argument de plus pour la transition post-quantique
 - Basé sur l'algorithme de Joux, Naccache et Thomé (2007)
 - 1 380 années-cœur de CPU sur cinq mois calendaires, avec 2^{32} requêtes à l'oracle
- Fondations remises en question : chiffrer != intégrer & factoriser n'est pas la seule voie

<https://www.theregister.com/security/2026/09/14/new-hardware-device-can-ram-into-encrypted-memory-expose-your-data/5296377>

<https://eprint.iacr.org/2026/2131>

■ Logitech Options+ : une souris qui donne les droits SYSTEM

- **[CVE-2026-12518]** le service de mise à jour tourne en NT AUTHORITY\SYSTEM
- Un utilisateur standard détourne ce service pour exécuter un installateur malveillant → SYSTEM, sans droits admin ni interaction
- Corrigé le 19 août (builds 2.7.954611 / 2.7.961922) — signalé... en mars
- Le logiciel « périphérique » anodin reste une vraie surface d'attaque sur le poste
<https://www.it-connect.fr/logitech-options-plus-faible-system-cve-2026-12518/>

Piratages, Malwares, spam, fraudes et DDoS



Piratages, Malwares, spam, fraudes et DDoS

Phishing / Microsoft 365

■ Microsoft 365 sous pression : le MFA contourné à la chaîne

- BigBear 2.0 (CloudSEK) : phishing-as-a-service AiTM (Evilginx2) qui rejoue le cookie de session
 - 258 organisations compromises, plus de 5 000 identifiants volés ; du JS désactive FIDO2 pour forcer un MFA plus faible
- Vishing « help desk » (PREY-0058, suivi par Microsoft depuis mai) : faux support IT par téléphone/Teams → tokens, puis cartographie via Microsoft Graph
- Parade : MFA résistant au phishing (FIDO2) + accès conditionnel sur appareil géré
<https://www.bleepingcomputer.com/news/security/bigbear-microsoft-365-phishing-service-bypassed-mfa-at-258-organizations/>
<https://thehackernews.com/2026/09/microsoft-365-attackers-use-help-desk.html>



Piratages, Malwares, spam, fraudes et DDoS

Opération / Démantèlement

■ EvilTokens démantelé : le premier PhaaS « IA à chaque étape »

- Plateforme de device-code phishing (Storm-2992), active depuis février 2026
 - Plus de 12 000 boîtes M365 dans plus de 10 000 organisations (dont la France)
 - La victime saisit elle-même un code sur le vrai site Microsoft → MFA contourné, puis une IA analyse la boîte et rédige la fraude
- 22 sept. : la DCU de Microsoft saisit 50 sites + 150 domaines (avec Cloudflare, Coinbase...)
- La Met Police (Londres) arrête 2 hommes (32 et 38 ans) le 11 sept.

<https://thehackernews.com/2026/09/microsoft-takes-down-eviltokens-device.html>

<https://www.theregister.com/security/2026/09/22/uk-cops-arrest-2-eviltokens-suspects-microsoft-seizes-50-phishing-kit-websites/5298317>

Piratages, Malwares, spam, fraudes et DDoS

Piratage

■ ShinyHunters s'en prend au FBI via Oracle PeopleSoft

- Le groupe affirme avoir exploité une 0-day PeopleSoft pour entrer dans les portails RH du FBI et voler les données d'agents (2-3 To revendiqués)
 - Portails emploi du FBI hors ligne ; l'agence confirme enquêter, Oracle silencieux
- En parallèle, Google/Mandiant alerte plus de 100 orgs : réexploitation de **[CVE-2026-35273]** (RCE non auth PeopleSoft), déjà utilisée en juin
 - La 0-day « inédite » ne vient que du pirate : prudence, pas de confirmation indépendante
- Arrestations côté police (dont un suspect présumé qui coopère)

<https://www.it-connect.fr/shinyhunters-piratage-fbi-oracle-peoplesoft-zero-day/>



CVE-2026-35273

Piratages, Malwares, spam, fraudes et DDoS

Pirater les pirates

■ Le pirate piraté : ShinyHunters rançonne le gang Clop

- ShinyHunters défigure le site Tor de fuite de Clop (« PWN3D BY SHINYHUNTERS »)
 - Entrée via une faille d'upload non authentifié du CMS Grav
- Clés privées Tor et logs revendiqués → rançon à 8 chiffres, « 2,333 % » de la valeur de Clop
 - Menace de publier la liste des entreprises ayant payé Clop (montants + adresses BTC)
- Guerre interne née de la campagne Oracle E-Business Suite (2025) et d'un exploit « emprunté »

<https://www.bankinfosecurity.eu/blogs/cyber-extortion-war-shinyhunters-holds-rival-clop-to-ransom-p-4192>



Piratages, Malwares, spam, fraudes et DDoS

Fraude / Fuite de données

■ **Revolut : des données arrachées via de fausses réquisitions « police italienne »**

- Le pirate (« IAmNotAVillain ») n'a pas percé Revolut : il a compromis des boîtes de la police italienne (infostealer) pour envoyer de fausses demandes légales
- Revolut aurait transmis les données d'environ 680 clients « crypto whales » (surtout Suisse et France), repérés par analyse on-chain
- 147 Go revendiqués côté forces de l'ordre italiennes ; rançon de 3 M\$ (6 000 XMR)
- Enquête du parquet de Reggio Calabria ; la CNIL italienne alerte les banques

<https://www.bankinfosecurity.eu/crypto-industry-figures-blackmailed-by-revoluts-hacker-a-32824>

Piratages, Malwares, spam, fraudes et DDoS

Malware / Supply chain

■ ClickFix partout : du fournisseur de confiance au compte vérifié

- Brevo : clé Cloudflare compromise → scripts injectés sur plus de 100 000 sites clients pendant ~5 h le 14 sept.
 - Leurre ClickFix pour les visiteurs + backdoor WordPress « Web Media Optimizer » si un admin était connecté
- HBO Max : compte Reddit vérifié piraté → 108 fausses pubs en 48 h (campagne PasteSwitch)
 - Fausse appli macOS, Codex... la victime colle elle-même la commande dans un terminal
- Rappel : ClickFix = plus de 50 % de l'activité des loaders en 2025. SRI + CSP côté défense
<https://www.it-connect.fr/brevo-attaque-supply-chain-clickfix-wordpress/>
<https://www.it-connect.fr/hbo-max-compte-reddit-pirate-clickfix-pasteswitch/>

Attaque Brevo (ClickFix)

11 100

Piratages, Malwares, spam, fraudes et DDoS

Malware

Téléchargements piégés : films, dépôts Git et extensions

- MovieReaper (Kaspersky) : itorrents.org compromis → un lien magnet renvoie un torrent piégé. Appât : « The Odyssey ». Relais C2 via la blockchain Solana
- FakeGit : 17 610 dépôts GitHub piégés pour diffuser SmartLoader puis le stealer StealC
- 16 extensions Firefox malveillantes imitant Rabby et OKX Wallet pour voler les cryptos

<https://www.it-connect.fr/moviereaper-malware-torrents-itorrents-the-odyssey/>

<https://www.it-connect.fr/fakegit-depots-github-smartloader-stealc/>



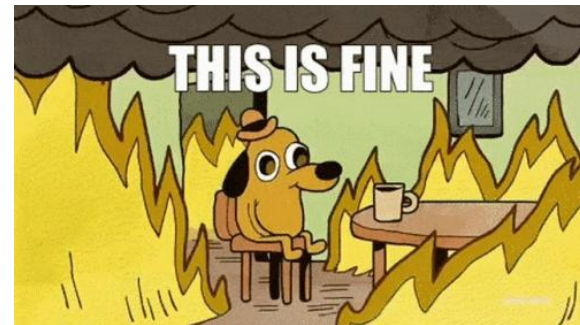
Piratages, Malwares, spam, fraudes et DDoS

Technique & outil

■ TryCloudflare : le tunnel gratuit devenu autoroute à RAT (le point annuel)

- TryCloudflare (try.cloudflare.com) crée un tunnel jetable, sans compte — pensé pour les devs
- Détourné en continu depuis 2024 : sous-domaine aléatoire en *.trycloudflare.com qui relaie vers le serveur de l'attaquant
 - Le trafic sort d'un service légitime → contournement du filtrage réseau
 - Charges typiques : AsyncRAT, XWorm, Remcos, VenomRAT (via LNK/VBS → scripts Python)
- Campagnes 2026 : SERPENTINE#CLOUD, AsyncRAT + Dropbox
- Défense : restreindre Python, surveiller *.trycloudflare.com

<https://www.securityweek.com/cloudflare-tunnels-abused-for-malware-delivery/>



Piratages, Malwares, spam, fraudes et DDoS

RSSI / France

■ État français : l'ANSSI passe à l'offensive (et balaie devant sa porte)

- REACTIV (demandé le 1er sept. par le PM) : l'ANSSI peut imposer aux ministères des mesures d'urgence dans des délais contraints
 - Point du 30 sept. : 99 violations signalées depuis le 1er août, 67 confirmées
- Faille Metabase : 9 instances ministérielles compromises — dont le labo d'innovation de l'ANSSI (118 comptes) et la DINUM
- Rapport DGFIP : attaque « pas sophistiquée » (identifiants volés, pas de MFA, pas de cloisonnement) et aucune des 2 vagues d'exfiltration détectée

<https://www.lemagit.fr/actualites/366650134/Une-veritable-autorite-de-lAnssi-en-cas-de-cyberattaque>

<https://www.it-connect.fr/rapport-anssi-cyberattaque-dgfip/>

Business et Politique



■ NIS 2 : enfin à l'ordre du jour... puis retiré

- Le projet de loi « Résilience » (transpose NIS 2, DORA, REC) était programmé à l'Assemblée à partir du 7 octobre
- La conférence des présidents l'a retiré de l'ordre du jour des 7 et 9 oct., sans nouvelle date
 - Toujours le même blocage : l'article 16 bis (interdiction des backdoors de chiffrement)
- Rappel : échéance de transposition dépassée depuis le 17 octobre 2024
- Pendant ce temps, les entreprises concernées se préparent quand même

<https://next.innk/brief-article/alleluia-la-transposition-de-nis2-est-enfin-a-lordre-du-jour-de-lassemblee-nationale/>

<https://projetarcadie.com/nis-2-de-nouveau-reporte/>

■ Cyber Resilience Act : la plateforme de signalement unique est en ligne

- ENISA a ouvert la Single Reporting Platform (SRP) le 11 septembre 2026
 - Même date que l'entrée en application des obligations de signalement (art. 14)
- Tout fabricant de produit « avec éléments numériques » signale les vulnérabilités activement exploitées et incidents graves via un seul portail
 - Notification sous 24 h / 72 h, rapport final sous 1 mois ; un CSIRT relaie ensuite
- Concret : Citrix a justement notifié ses 0-day NetScaler au titre du CRA
- Les rapports volontaires sur les vulnérabilités, les cybermenaces, les incidents et les quasi-accidents au titre de l'article 15 sont prévus pour une phase ultérieure

<https://www.helpnetsecurity.com/2026/09/14/enisa-cra-single-reporting-platform/>

■ CNIL : 500 000 € pour l'Hôpital privé de la Loire

- Fuite de l'été 2025 : 524 867 patients + 202 246 « tiers de confiance » (727 000 personnes)
- Un seul compte (d'un praticien externe) a pu lire les dossiers de TOUS les patients
 - Reproches CNIL (art. 32 & 34 RGPD) : pas de cloisonnement, pas de MFA, accès permanent laissé à l'éditeur, tiers de confiance non informés
- Montant calculé au poids du groupe Ramsay Santé ; soit environ 0,69 € par personne

<https://www.bleepingcomputer.com/news/security/french-hospital-fined-500-000-after-breach-exposes-data-of-727-000/>

Conférences



Conférences

Octobre – novembre 2026

Passées

No Hat

10 oct. · Bergame (Italie)

Pwn2Own Ireland

6-9 oct. · Cork

À venir

Hexacon

16-17 oct. · Paris (Palais Brongniart)

ETSI

19-22 oct. · Sophia Antipolis

hack.lu

20-23 oct. · Luxembourg

UYBHYS

6-7 nov. · Brest

GreHack

13 nov. · Grenoble

DeepSec

17-20 nov. · Vienne (Autriche)

Divers / Trolls velus



■ Windows 11 26H2 : beaucoup de bruit pour un nouveau compteur de support

- Disponible depuis le 29 septembre 2026, via un simple enablement package (174 Ko)
- Aucune nouveauté exclusive : regroupe les fonctions déployées dans l'année
- Le vrai intérêt : relancer le cycle de support
 - 24 mois Famille/Pro (→ oct. 2028), 36 mois Entreprise/Édu (→ oct. 2029)
- Tombe à pic : le support de 24H2 (Famille/Pro) se termine... aujourd'hui, 13 octobre

<https://www.it-connect.fr/windows-11-26h2-disponible-mise-a-jour-2026/>

Divers / Trolls velus

Divers

■ Le compte X officiel de Microsoft piraté... pour un token Clippy

- 1er oct. : le compte @Microsoft (13 M d'abonnés) détourné une trentaine de minutes
- Photo changée en Clippy, repartage d'un faux compte « retour de Clippy »
- But : profiter de la crédibilité du compte pour pousser un token \$Clippy, prétendument « lié à \$MSFT »
- Fausses excuses publiées puis supprimées. Microsoft a fini par reprendre la main
- Rappel : aucune entreprise cotée ne lie son ticker à un token lancé par des inconnus

<https://www.it-connect.fr/compte-x-microsoft-pirate-clippy-crypto/>



■ Pwn2Own Ireland 2026 : le Galaxy S26 tombe en boucle

- Ouverture le 6 octobre à Cork ; record de tentatives sur smartphones
- Jour 1 : 32 zero-day, 388 500 \$; le Galaxy S26 piraté plusieurs fois
 - Ikotas : RCE à distance « avec un simple e-mail » (toucherait aussi le Pixel 10)
- Jour 2 : encore 3 compromissions du Galaxy S26
- « Collisions » : des failles déjà connues de Samsung fonctionnent encore = patch pas déployé

<https://www.it-connect.fr/pwn2own-ireland-2026-samsung-galaxy-s26-pirate/>

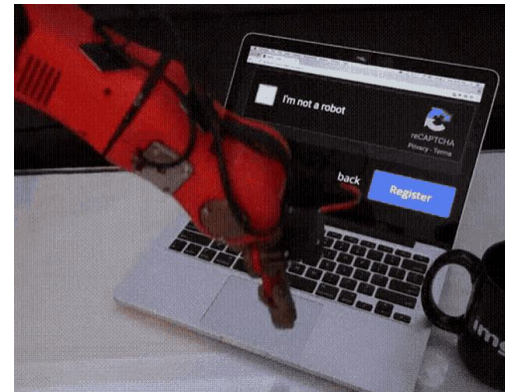
Divers / Trolls velus

Divers

« Je ne suis pas un robot » : GPT-6 Astra valide les 48 niveaux

- Un ingénieur OpenAI fait jouer le modèle au jeu « I'm Not a Robot » (neal.fun)
- 48 niveaux de captchas variés enchaînés sans échec visible → « certificat d'humain »
 - Pas un captcha commercial live, mais une vraie démo de « Computer Use » (clic, glisser, règles changeantes)
- Le captcha image seul, c'est fini : Google/Cloudflare misent déjà sur le comportement (Turnstile, reCAPTCHA v3)

<https://www.numerama.com/tech/2326999-je-ne-suis-pas-un-robot-gpt-6-astra-a-valide-les-48-niveaux-dun-jeu-de-captchas-concus-pour-sarracher-les-cheveux.html>



Prochaine réunion ?

- RDV le mardi 10 novembre 2026

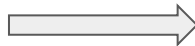


Accéder aux différents supports ?



Replays

Slides



<https://www.youtube.com/@OSSIR>

<https://www.ossir.org/support-des-presentations/>