Revue d'actualité de l'OSSIR

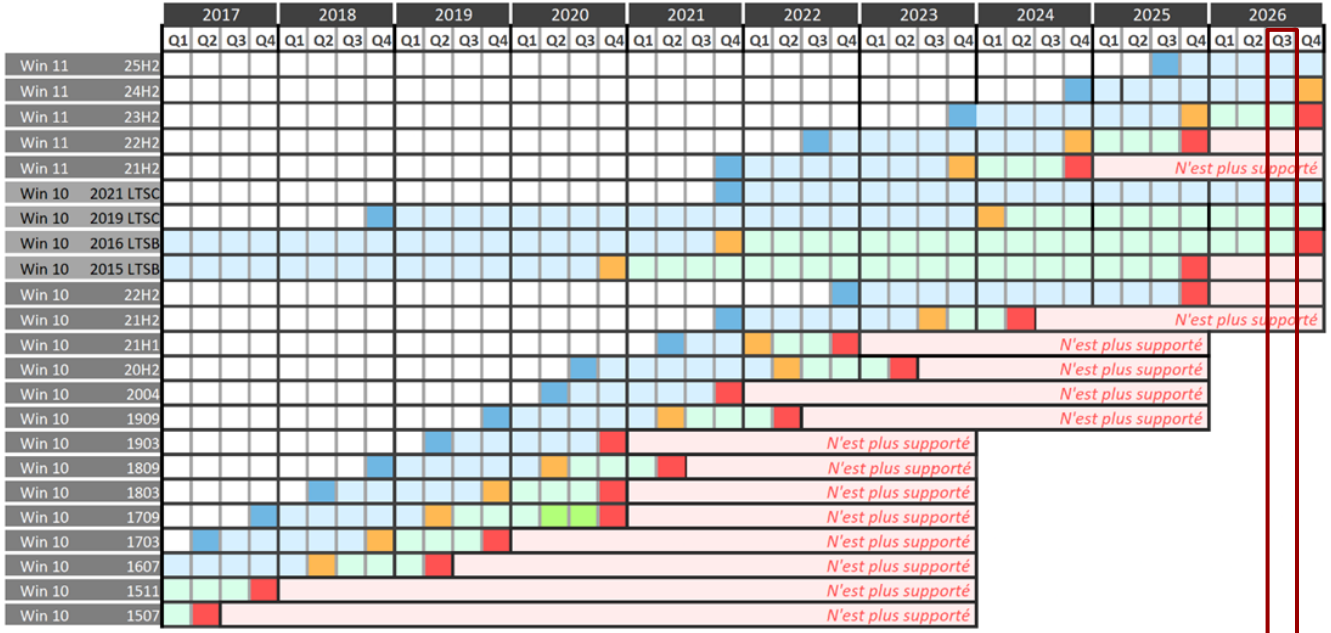
8 septembre 2026

Jérémy De Cock
Melchior Courtois

<< La veille vous est fournie par cyberzen *>>*

Rappel du support Windows en couleurs

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Workstation***



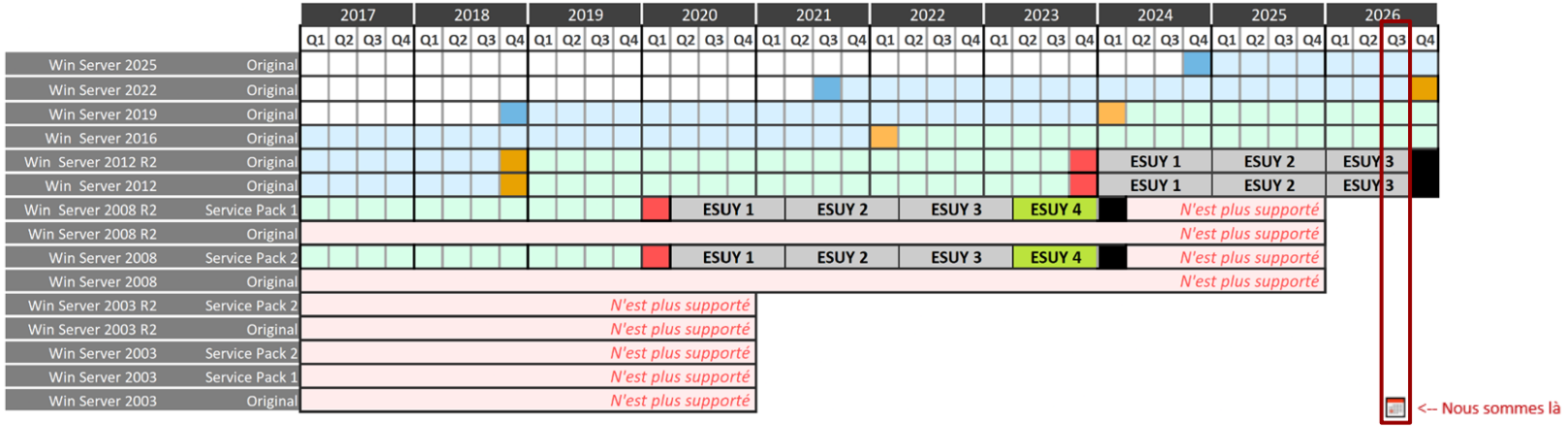
Sortie	Home, Pro	Entreprise
mardi 30 septembre 2025	mardi 12 octobre 2027	mardi 10 octobre 2028
mardi 1 octobre 2024	mardi 13 octobre 2026	mardi 12 octobre 2027
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 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	jeudi 13 juillet 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

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 LTSB/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 LTSB/LTSC

LTSB : **L**ong-**T**erm **S**ervicing **B**ranch
LTSC : **L**ong-**T**erm **S**ervicing **C**hannel

Failles / Bulletins / Advisories (MMSBGA)
Microsoft - Windows ***Server***



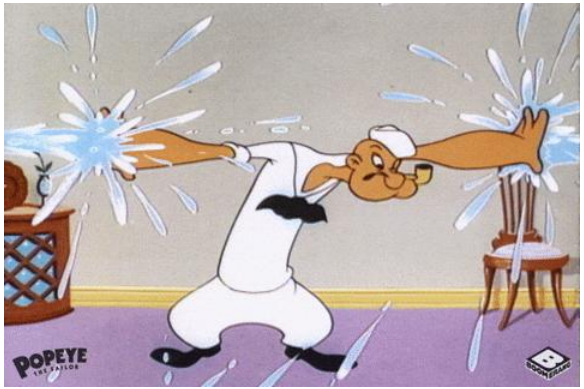
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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

ESYC : **E**xtended **S**ecurity **U**pdate **Y**ear

Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Patch Tuesday de juin : 200 failles, dont 3 zero-day

- Publié le 9 juin — 200 vulnérabilités, dont 33 critiques
  - Volume dopé par MDASH, le système multi-agents IA de Microsoft
- 3 zero-day, déjà divulguées publiquement mais pas encore exploitées
  - **[CVE-2026-45586]** élévation de privilèges dans CTFMON — CVSS 7,8
    - Composant de gestion des saisies clavier / langues : accès local → SYSTEM
    - Divulguée par Nightmare Eclipse
  - **[CVE-2026-49160]** déni de service dans HTTP.sys via HTTP/2 — CVSS 7,5
    - C'est HTTP/2 Bomb, présentée dans la revue de juin
  - **[CVE-2026-50507]** contournement de BitLocker
    - Alias YellowKey, toujours Nightmare Eclipse
- À regarder aussi :
  - 11 failles dans le client Bureau à distance, dont 7 critiques
  - **[CVE-2026-42897]** Exchange activement exploitée — le 1er correctif avait été contourné

https://www.lemondeinformatique.fr/actualites/lire-patch-tuesday-juin-2026-plus-de-200-failles-corrigees-100420.html
https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2026-patch-tuesday-fixes-6-zero-days-200-flaws/
https://www.it-connect.fr/patch-tuesday-juin-2026-200-failles-de-securite-patchees-dont-3-zero-day/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Patch Tuesday de juillet : le plus gros de l'histoire de Microsoft

- Publié le 14 juillet — 570 vulnérabilités, dont 57 critiques
  - Presque 3× le record du mois précédent
  - Microsoft assume : découverte assistée par IA sur le code de Windows
- 3 zero-day, dont 2 déjà exploitées
  - **[CVE-2026-56155]** élévation de privilèges dans AD FS — exploitée
    - Trouvée par le DART de Microsoft, donc probablement en réponse à incident
    - AD FS = brique d'identité hybride, le pivot rêvé une fois dans la place
  - **[CVE-2026-56164]** élévation de privilèges SharePoint — exploitée, à distance et sans authentification
    - Ajoutée au KEV de la CISA dès le 14 juillet
    - Si vous ne pouvez pas patcher : AMSI + analyse du corps de requête en mode Full
  - **[CVE-2026-50661]** contournement de BitLocker, divulgué par un chercheur « anonyme »
    - Après YellowKey et GreatXML, on a une petite idée du nom
- Et aussi : phase finale du durcissement Kerberos — RC4, c'est terminé

https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2026-patch-tuesday-fixes-massive-570-flaws-3-zero-days/
https://securityonline.info/july-2026-patch-tuesday/
https://www.it-connect.fr/patch-tuesday-juillet-2026-570-failles-de-securite-corrigees-dont-3-zero-day/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Patch Tuesday d'août : 421 failles et un rootkit nord-coréen

- Publié le 11 août — 421 vulnérabilités, dont 62 critiques
- 3 zero-day
  - **[CVE-2026-68820]** use-after-free dans afd.sys (WinSock) — CVSS 7,0, exploitée
    - Race condition : un compte local authentifié devient SYSTEM, sans interaction
    - Attribuée à Lazarus par Check Point — campagne Operation Dream Job
    - Sert à déployer FudModule (rootkit noyau) et la backdoor ForestTiger
    - Échantillon compilé le 7 juillet : des semaines d'exploitation avant le patch
  - **[CVE-2026-62832]** User Profile Service, suivi de lien → administrateur
    - C'est LegacyHive, encore signée Nightmare Eclipse
  - **[CVE-2026-72971]** pilote unionfs.sys, isolation des conteneurs Windows
- La vraie urgence du mois : **[CVE-2026-62878]** RCE non authentifiée dans le DNS Windows
  - CVSS 9,8 et jugée « wormable » par la ZDI

https://www.securityweek.com/august-2026-patch-tuesday-microsoft-fixes-421-cves-one-exploited-zero-day/
https://www.theregister.com/security/2026/08/11/421-bugs-in-microsofts-patch-tuesday-release-and-the-norks-have-already-attacked-one/
https://www.it-connect.fr/patch-tuesday-aout-2026-421-failles-corrigees-3-zero-day/

Failles / Bulletins / Advisories
Système

GreatXML : YellowKey à peine corrigée, BitLocker retombe

- Microsoft corrige YellowKey dans le Patch Tuesday de juin...
  - Et quelques heures plus tard, une nouvelle zero-day BitLocker est publiée
- Baptisée GreatXML, toujours signée Nightmare Eclipse
  - Le chercheur avait promis « une grande surprise » pour juin : promesse tenue
- Elle a probablement été corrigée en juillet sous **[CVE-2026-50661]**
  - Microsoft crédite « un chercheur anonyme »... on vous laisse deviner

https://www.it-connect.fr/faille-greatxml-contournement-bitlocker-windows-zero-day/

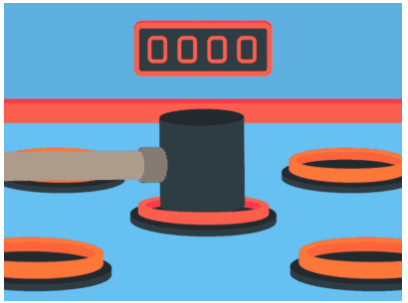
Failles / Bulletins / Advisories
Système

RoguePlanet : la saga Defender en trois épisodes

CVE-2026-50656

- 11 juin — publication de la zero-day, quelques heures après le Patch Tuesday
  - Cible Windows Defender et donne les privilèges SYSTEM
  - Fonctionne sur un Windows 11 totalement à jour (KB5094126 incluse)
  - Et même sur les versions Canary de Windows, d'après le chercheur
- 9 juillet — Microsoft corrige, **[CVE-2026-50656]**
- 10 juillet — le chercheur remet une pièce dans la machine
  - Selon lui, le correctif permet un déni de service en saturant le disque local
- 18 août — le patch est contourné : voir la slide suivante

https://www.it-connect.fr/windows-rogueplanet-une-faille-zero-day-devoilee-juste-apres-les-mises-a-jour-de-juin/
https://www.it-connect.fr/microsoft-corrige-faille-zero-day-rogueplanet-defender/
https://www.it-connect.fr/windows-defender-patch-rogueplanet-effets-de-bord/



Failles / Bulletins / Advisories
Système

ShieldBreak : le patch RoguePlanet contourné

CVE-2026-69414

- Zero-day publiée par... Nightmare Eclipse (oui, encore)
- Contourne purement et simplement le correctif RoguePlanet de Defender
- Microsoft déclare travailler sur un correctif
  - Épisode 4 attendu pour le prochain Patch Tuesday ?

https://www.it-connect.fr/shieldbreak-zero-day-defender-cve-2026-69414/

0-DAY
aucun correctif

Failles / Bulletins / Advisories
Système

L'été des élévations de privilèges Linux

- **[CVE-2026-23111]** — une erreur de syntaxe d'un seul caractère dans le noyau
- DirtyClone **[CVE-2026-43503]** — noyau, root sur Debian, Ubuntu et Fedora
- GhostLock **[CVE-2026-43499]** — présente depuis 2011, la majorité des distributions
  - Découverte à l'aide d'une IA
- snap-confine **[CVE-2026-8933]** — root local sur Ubuntu
- RefluXFS **[CVE-2026-64600]** — système de fichiers XFS, RHEL / CentOS / AlmaLinux
- Bad Epoll **[CVE-2026-46242]** — Linux et Android
  - Et que l'IA Mythos, elle, avait laissé passer
- Six privesc locales en trois mois : le durcissement des postes reste d'actualité

https://www.it-connect.fr/linux-une-faille-permet-de-devenir-root-a-cause-dun-unique-caractere/
https://www.it-connect.fr/dirtyclone-la-faille-linux-qui-donne-un-acces-root-en-silence/
https://www.it-connect.fr/ghostlock-faille-linux-acces-root/
https://www.it-connect.fr/cve-2026-8933-ubuntu-snap-confine-acces-root/
https://www.it-connect.fr/refluxfs-cve-2026-64600-faille-xfs-acces-root-linux/
https://www.it-connect.fr/bad-epoll-faille-noyau-linux-android-acces-root/

Failles / Bulletins / Advisories
Système

Januscape : 16 ans dans l'ombre au cœur de KVM

CVE-2026-53359

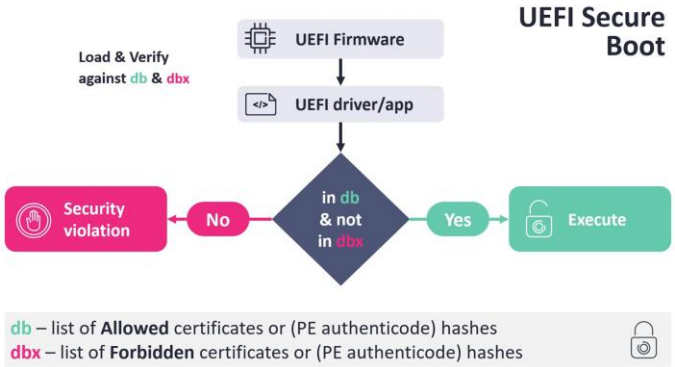
- Use-after-free resté 16 ans dans KVM, l'hyperviseur du noyau Linux
- Une VM peut planter son hôte, voire s'en évader
  - Aussi bien sur Intel que sur AMD
- Pourquoi c'est un sujet : l'évasion de VM casse la séparation entre clients
  - Sur un hôte mutualisé, un locataire peut atteindre les autres

https://www.it-connect.fr/januscape-faille-kvm-evasion-vm-hote/

Failles / Bulletins / Advisories
Système

Secure Boot : 11 shims signés Microsoft, jamais révoqués

- Identifiés par ESET
- Un shim = le petit binaire signé par Microsoft qui amorce un bootloader tiers
  - Il porte la confiance de la clé Microsoft, d'où l'intérêt pour un attaquant
- Copier l'un de ces 11 binaires suffisait à contourner Secure Boot
  - Sur Linux comme sur Windows
- Le problème n'est pas la faille, c'est la révocation (dbx) qui n'a jamais suivi
  https://www.it-connect.fr/secure-boot-11-shims-signes-microsoft-eset/



Failles / Bulletins / Advisories
Système


CVE-2026-54121

Certighost : un compte AD standard suffit pour usurper un DC

- Faille dans AD CS, l'autorité de certification intégrée à l'Active Directory
  - Principe des attaques ESC : obtenir un certificat au nom d'un autre compte
  - Ici, un utilisateur standard peut se faire passer pour un contrôleur de domaine
- = compromission du domaine, sans mot de passe d'administrateur
- Si vous avez une PKI AD, c'est le moment de repasser sur vos templates
  https://www.it-connect.fr/certighost-cve-2026-54121-ad-cs-controleur-de-domaine/

Failles / Bulletins / Advisories
Système

CVE-2026-27912

ResetNightmare : Kerberos rend les armes

- Permet de réinitialiser le mot de passe de n'importe quel compte Active Directory
  - Y compris les comptes à privilèges
- = prise de contrôle du domaine
- À surveiller côté détection : les événements 4724 / 4738 inattendus

https://www.it-connect.fr/resetnightmare-cve-2026-27912-kerberos-active-directory/

Failles / Bulletins / Advisories
Système


CVE-2026-69836

Entra ID : CVSS 10, déjà exploitée, et vous n'avez rien à faire

- Faille critique dans Entra ID (RCE), exploitée dans la nature
- Corrigée côté Microsoft
  - Service cloud = correctif appliqué globalement, aucune action client
- Le revers de la médaille : vous n'avez pas non plus le choix du calendrier
  - Ni la visibilité sur la fenêtre d'exposition

https://www.it-connect.fr/entra-id-cve-2026-69836-faille-cvss-10-exploitee/

Failles / Bulletins / Advisories
Système


CVE-2026-47876

VMware : 3 failles critiques dans vCenter et ESX

- Broadcom a dévoilé 5 vulnérabilités le 29 juillet 2026
- Dont 3 critiques
  - **[CVE-2026-47876]** évasion de machine virtuelle
- Le classique de l'été chez VMware
  - Rappel : vCenter compromis = tout le cluster compromis

https://www.it-connect.fr/vmware-3-failles-critiques-vcenter-esx-juillet-2026/

Failles / Bulletins / Advisories
Système

Proxmox VE 7 : root sans mot de passe sur les hôtes oubliés


CVE-2023-54391

- Avis PSA-2026-00043-1 publié le 1er septembre — CVSS 9,8
  - Exploitée dans la nature, PoC public, hôtes chiffrés depuis fin août
  - Le paramètre tfa-challenge court-circuite la vérification du mot de passe
  - L'attaquant présente une requête 2FA indiquant au serveur que le mot de passe a déjà été donné
  - Sur un compte sans 2FA, le challenge n'est jamais validé mais l'authentification est autorisée : ticket root@pam
- Ce n'est pas un 0day, mais un n-day
  - Corrigée en juillet 2023 dans libpve-access-control 8.0.4… sans CVE ni advisory
  - PVE 7.x est en fin de vie depuis juillet 2024 : ce sont les hôtes oubliés qui tombent
- Ransomwares et cryptomineurs, avec effacement des traces
  - Journaux remplacés par des liens vers /dev/null, /var/lib/dpkg/status détruit
- Trois réflexes : sortir le port 8006 d'Internet, 2FA sur root@pam, quitter la 7.x
  - Un compte protégé par un second facteur n'est pas contournable par cette faille

https://flawfence.com/blog/proxmox-ve-7-faille-authentification-rce-cve-2023-54391/
https://securityonline.info/proxmox-ve-7-auth-bypass-poc-exploited/

Failles / Bulletins / Advisories
Système

Apple : deux vagues de correctifs cet été

- 2 juillet — iOS, iPadOS et macOS Tahoe 26.5.2
  - Plus de 30 failles, dont 4 trouvées via l'IA
  - Correctifs livrés plus tôt que prévu
- 29 juillet — plus de 200 failles sur l'ensemble des systèmes
  - Contournements de Gatekeeper, accès root sur macOS, faille dans le noyau
  - Aucun zero-day, mais 11 failles découvertes avec l'IA
- Même tendance que chez Microsoft et Google : le volume explose

https://www.it-connect.fr/apple-corrige-plus-de-30-failles-sur-ios-et-macos-decouvertes-en-partie-avec-lia/
https://www.it-connect.fr/apple-plus-de-200-failles-patchees-tous-ses-systemes/

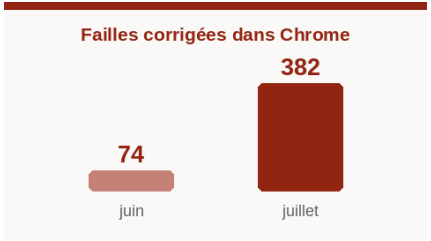
Failles / Bulletins / Advisories
Navigateur (principales failles)

Chrome : 74 failles en juin, 382 en juillet

CVE-2026-11645

- 10 juin — 74 vulnérabilités corrigées
  - **[CVE-2026-11645]** zero-day déjà exploitée
- 3 juillet — Chrome 151 corrige 382 failles d'un seul coup, dont 15 critiques
  - Un record, largement porté par l'IA
- Conséquence pratique : le cycle de mise à jour navigateur ne se néglige plus
  - Et pensez à forcer le redémarrage du navigateur, sinon le patch ne s'applique pas

https://www.it-connect.fr/google-chrome-74-vulnerabilites-patchees-dont-une-faille-zero-day-deja-exploitee/
https://www.it-connect.fr/google-chrome-151-382-failles-corrigees-ia/



Failles / Bulletins / Advisories
Navigateur (principales failles)

Firefox : quand l'IA du navigateur vide votre boîte mail

- Injection de prompt depuis un site piégé
  - Le site pousse l'IA intégrée à Firefox à exfiltrer les e-mails de l'utilisateur
  - Scénario réalisé par un chercheur chez ERNW
- Faille atténuée par Mozilla
  - « Atténuée », pas « corrigée » — nuance importante
- Le fond du problème : un LLM ne distingue pas ses instructions du contenu qu'il lit
  - Donc tout contenu affiché devient une entrée de commande potentielle

https://www.it-connect.fr/cette-faille-de-firefox-transformait-lia-en-complice-du-vol-de-vos-e-mails/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)


CVE-2026-42824

Copilot : deux exfiltrations en un clic

- 16 juin — SearchLeak **[CVE-2026-42824]**, sur Copilot Enterprise
  - Une URL piégée suffit à faire sortir e-mails, fichiers OneDrive et SharePoint
- 20 août — CoSnitch **[CVE-2026-24301]**, sur Copilot Personal
  - Un clic, et l'assistant exfiltre les e-mails
  - La partie amusante : ce sont les chercheurs qui ont interrogé l'IA...
    - ... et l'IA leur a décrit sa propre faille
- Deux fois le même schéma : l'assistant a vos droits, il suffit de le téléguider

https://www.it-connect.fr/searchleak-la-faille-qui-transformait-copilot-en-outil-de-vol-de-donnees-en-un-clic/
https://www.it-connect.fr/cosnitch-cve-2026-24301-copilot-personal-faille-un-clic/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

GLPI : deux vagues de correctifs en une semaine

- 25 juin — GLPI 11.0.8 et 10.0.26
  - 16 vulnérabilités patchées dans GLPI 11, dont 2 critiques
    - Une RCE et un contournement du MFA
- 29 juin — les plugins communautaires
  - 15 failles, dont une RCE critique (CVSS 8,9) dans GenericObject
- Le réflexe : patcher les plugins, pas seulement le cœur
  - Et faire le ménage dans ceux qui ne servent plus

https://www.it-connect.fr/glpi-11-0-8-et-10-0-26-16-failles-patchees-dont-2-critiques/
https://www.it-connect.fr/plugins-glpi-15-failles-patchees-dont-une-rce-critique/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)


CVE-???

wp2shell : le cœur de WordPress en RCE pré-authentifiée

- Pas un plugin, pas un thème : le cœur du CMS
  - Dans son API Rest
- Exécution de code à distance, sans authentification
- Concerne les versions 6.9 et 7.0
- Face à l'urgence, les mises à jour ont été forcées
  - Des millions de sites concernés (500M ?)
- Première victime notable : le site officiel de Nextcloud (19/07)
  - nextcloud.com est resté hors ligne, défacement reconnu par l'éditeur
  - Le site vitrine, pas le produit — mais l'effet d'image est le même

https://www.it-connect.fr/wordpress-wp2shell-rce-critique-coeur-cms/
https://www.it-connect.fr/nextcloud-site-officiel-piratee-defacement-wp2shell/

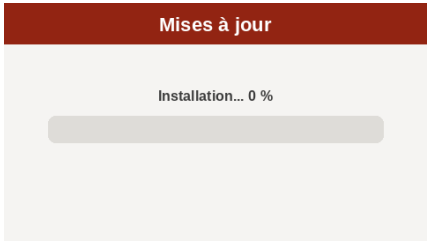
Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

7-Zip 26.02 : à installer à la main

CVE-2026-14266

- Débordement de tampon dans le décodage XZ
- Pas de mise à jour automatique dans 7-Zip : l'installation reste manuelle
  - Donc à pousser via votre outil de déploiement
- Le genre de logiciel qui traîne en version 21.x sur la moitié du parc

https://www.it-connect.fr/7-zip-26-02-faille-rce-cve-2026-14266/



Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

SharedRoot : l'agent IA de Claude Cowork s'évade de sa VM

- Des chercheurs ont fait sortir l'agent de sa machine virtuelle
  - Lecture ET écriture sur le Mac hôte
- Anthropic n'a pas publié de correctif
- Le sujet de fond : les agents IA tournent avec les droits de l'utilisateur
  - La sandbox est la seule barrière — quand elle tombe, il ne reste rien

https://www.it-connect.fr/sharedroot-claude-cowork-evasion-sandbox-mac/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

GitLab : exploitée deux jours après le correctif


CVE-2026-19478

- Faille critique corrigée par GitLab
  - Injection de code via une directive GraphQL
  - Sans authentification requise !
- 48 h plus tard : tentatives d'exploitation constatées
- La fenêtre entre patch et exploitation continue de se réduire
  - Un GitLab, c'est aussi vos secrets CI et vos clés de déploiement

https://www.it-connect.fr/gitlab-cve-2026-19478-faille-critique-exploitee/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

CVE-2026-18963

Keycloak : le « mot de passe oublié » un peu trop généreux

- Permet de réinitialiser le mot de passe de n'importe quel compte
  - Sans authentification préalable
- Sur un fournisseur d'identité, l'impact se passe de commentaire
  - Une seule faille et c'est tout le SSO qui tombe
- Un patch est disponible

https://www.it-connect.fr/keycloak-cve-2026-18963-faille-critique-mot-de-passe-oublie/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

Zimbra : 274 serveurs de messagerie déjà compromis

CVE-2026-73570

- Injection de commande dans le composant de supervision SNMP — CVSS 8,9
  - Requête SMTP forgée, aucune authentification, code exécuté en tant qu'utilisateur zimbra
- Trois conditions pour être vulnérable :
  - Paquet optionnel zimbra-snmp installé
  - Notifications SNMP activées (snmp_notify)
  - Service swatchdog démarré — actif par défaut
- Chronologie : divulguée le 26 juin, corrigée le 20 juillet dans ZCS 10.1.20
  - CERT Polska signale l'exploitation active le 17 août, la CISA l'ajoute au KEV le 21
  - Shadowserver compte 274 instances compromises le 22 août — et 8.200 non patchées
- La France est le 3e pays le plus touché, derrière les États-Unis et la Suède

https://www.bleepingcomputer.com/news/security/hackers-breached-over-270-zimbra-servers-in-ongoing-attacks/
https://thehackernews.com/2026/08/attackers-exploit-zimbra-snmp-flaw-for.html
https://www.it-connect.fr/zimbra-cve-2026-73570-serveurs-compromis/

Failles / Bulletins / Advisories
Application / Framework / … (principales failles)

Next.js : deux RCE critiques, dont une via une image AVIF

CVE-???
CVE-2026-75604

- Corrigées par Vercel
- Exécution de code à distance via une image AVIF piégée (pour libheif), sans authentification
  - L'upload d'image devient le point d'entrée
- Traversée de répertoire sur les serveurs Windows

https://www.it-connect.fr/nextjs-failles-critiques-avif-windows-rce/

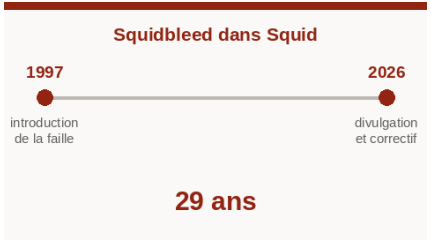
Failles / Bulletins / Advisories
Réseau (principales failles)

Squidbleed : 29 ans de fuite dans le proxy Squid

CVE-2026-47729

- Présente depuis 1997
- Permet de lire en clair les requêtes HTTP des autres utilisateurs du proxy
  - Donc les identifiants et jetons qui transitent dedans
  - Type « heap over-read »
- Un proxy mutualisé devient un point d'écoute pour n'importe quel utilisateur

https://www.it-connect.fr/squidbleed-faille-proxy-squid-cve-2026-47729/



Failles / Bulletins / Advisories
Réseau (principales failles)


CVE-2026-42533

NGINX : la regex qui fait tomber le worker

- Faille critique corrigée par F5
- Située dans la directive map avec expressions régulières
- Fait planter les workers, et parfois permet une exécution de code à distance
  - Deuxième grosse faille NGINX de l'année après NGINX Rift en juin

https://www.it-connect.fr/nginx-cve-2026-42533-faille-critique-map-regex/

Failles / Bulletins / Advisories
Réseau (principales failles)

Citrix NetScaler : contournement d'authentification à distance


CVE-2026-19490

- Deux vulnérabilités corrigées dans NetScaler ADC et Gateway
- **[CVE-2026-19490]** ouvre la porte à un contournement de l'authentification, à distance
- Équipement de bordure exposé : à traiter en priorité absolue
  - Historiquement, les NetScaler sont scannés dans les heures qui suivent l'avis

https://www.it-connect.fr/citrix-netscaler-cve-2026-19490-contournement-authentification/

Failles / Bulletins / Advisories
Réseau (principales failles)

UniFi : 22 failles, dont 3 à 10 sur 10

- Bulletin Ubiquiti d'août 2026
- 22 vulnérabilités sur l'écosystème : Protect, Network, OS et Talk
- 3 failles critiques avec un score CVSS de 10 sur 10
  - Le maximum : exploitable à distance, sans authentification, impact total
- Deuxième bulletin sévère de l'année après celui de juin sur UniFi OS Server

https://www.it-connect.fr/ubiquiti-bulletin-aout-2026-failles-unifi/

Failles / Bulletins / Advisories
Autre (principales failles)

FatFs : 7 failles sans correctif dans des millions d'objets

- FatFs = implémentation FAT embarquée dans une quantité d'objets connectés
- Sept vulnérabilités, aucune corrigée
- Le vrai problème : c'est difficile à patcher
  - Code figé dans le firmware, fabricants disparus, pas de canal de mise à jour
- Le péché originel de l'IoT, une fois de plus

https://www.it-connect.fr/fatfs-sept-failles-sans-correctif-appareils-iot/

Failles / Bulletins / Advisories
Autre (principales failles)

GPUThor : le Rowhammer qui casse l'ECC des GPU NVIDIA

- Université de Toronto, présentation prévue à ACM CCS 2026
- Rowhammer sur GDDR6 : jusqu'ici l'ECC suffisait, ce n'est plus le cas
  - Deux comportements non documentés retrouvés par rétro-ingénierie
    - La fusion des accès mémoire se contourne en jouant sur les warps
    - Le TRR n'intervient qu'une fois sur 72 rafraîchissements — donc prévisible
- Résultat : 6,6× plus de coups portés, et des milliers de bits qui basculent
  - Trouver un bit exploitable : 21,9 h avec GPUHammer → 1,1 minute
- Avec l'ECC actif : reboot du GPU toutes les 2 h, et surtout shell root sur l'hôte
  - Via corruption des pagetables depuis un programme CUDA non privilégié
- RTX A4000, A4500, A5000 et A6000 — bulletin NVIDIA du 21 août

https://gputhor.com/
https://nvidia.custhelp.com/app/answers/detail/a_id/5873
https://www.it-connect.fr/gputhor-attaque-rowhammer-ecc-gpu-nvidia/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Tchap : un pirate s'invite sur la messagerie chiffrée de l'État

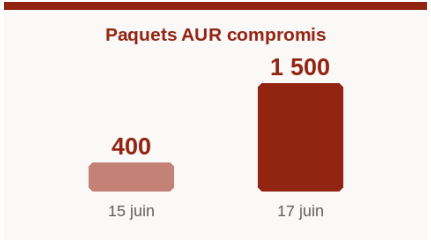
- Messagerie instantanée réservée aux agents publics français
- Intrusion via la compromission du compte d'un agent
  - Pas de faille dans le chiffrement : un compte, tout simplement
- Le chiffrement de bout en bout ne protège pas d'un terminal légitime compromis
  https://www.it-connect.fr/cyberattaque-tchap-un-pirate-sest-introduit-sur-la-messagerie-chiffree-de-letat/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Arch Linux : l'AUR pris d'assaut, deux fois

- 15 juin — plus de 400 paquets de l'AUR compromis
  - Diffusion d'un rootkit et d'un infostealer
  - Cible : les identifiants des développeurs
- 17 juin — la vague monte à plus de 1.500 paquets
  - Arch bloque la création de comptes le temps de nettoyer
- Rappel : l'AUR n'a jamais prétendu être un dépôt de confiance
  - N'importe qui y publie, le PKGBUILD s'exécute avec vos droits

https://www.it-connect.fr/arch-linux-plus-de-400-paquets-de-laur-pieges-par-un-rootkit-et-un-infostealer/
https://www.it-connect.fr/aur-plus-de-1-500-paquets-compromis-arch-linux-ferme-les-inscriptions/



Piratages, Malwares, spam, fraudes et DDoS
Piratage

OptinMonster : 1,2 million de sites WordPress exposés

- Attaque de type supply chain
  - CDN officiel des extensions (clé API compromise)
  - Issue de la post-exploitation d'une faille dans l'extension UpdraftPlus
- Trois produits du même éditeur visés : OptinMonster, TrustPulse et PushEngage
- Plus de 1,2 million de sites WordPress exposés
  - Un éditeur compromis = tous ses clients compromis, en une mise à jour

https://www.it-connect.fr/wordpress-1-2-million-de-sites-exposes-apres-le-piratage-doptinmonster/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Coupe du monde : une inscription d'agent ouvrait les flux TV mondiaux

- Il suffisait de s'inscrire comme agent de football
  - Sur agents.fifa.org (pour info)
- Accès aux systèmes de production de la Coupe du monde 2026 :
  - Flux TV, scores, commentaires (merci fdp.fifa.org)
  - Broken Access Control !
- Possibilité de remplacer le flux principal et/ou de gérer les matchs ⚽
  - Aucun moyen de signaler la faille, pas de VDP ni de programme de bug bounty
  - Une nuit passée à envoyer des mails et à appeler des personnes
    - Il a fallu joindre la CISA et le FBI..
- Un cloisonnement d'habilitations inexistant entre un portail public et la prod

https://www.it-connect.fr/coupe-du-monde-2026-une-faille-fifa-permettait-de-detourner-les-flux-tv-mondiaux/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Le Wi-Fi des hôtels détourné pour siphonner Microsoft 365

- Des passerelles Wi-Fi d'hôtels sont compromises
- Empoisonnement DNS depuis la passerelle
  - Les voyageurs sont redirigés vers de faux portails Microsoft 365
- À rappeler avant les déplacements : VPN d'entreprise systématique
  - Et méfiance sur les portails captifs qui redemandent une authentification

https://www.it-connect.fr/wifi-hotel-dns-poisoning-microsoft-365/

Piratages, Malwares, spam, fraudes et DDoS
Phishing / Fraude

DEBULL : le device code Microsoft 365 détourné

- Kit de phishing repéré par ZeroBEC
- Abuse du device code flow de Microsoft
  - Prévu pour les appareils sans clavier — TV, imprimantes, IoT
  - La victime saisit elle-même un code sur le vrai site Microsoft
- Résultat : compte M365 piraté sans jamais voler le mot de passe, MFA contourné
  - À bloquer via une stratégie d'accès conditionnel dédiée

https://www.it-connect.fr/debull-device-code-phishing-microsoft-365/

Piratages, Malwares, spam, fraudes et DDoS
Phishing / Fraude

L'arnaque FaceTime qui vide les comptes en direct

- Les escrocs se font passer pour la banque ou le support Apple
- Appel FaceTime, puis partage d'écran
  - Captation en direct des identifiants et des codes bancaires
- À faire passer à vos parents
  https://www.it-connect.fr/arnaque-facetime-appel-video-comptes-bancaires/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Steam : des wallpapers animés qui installent bien plus que du décor

- Campagne révélée par Kaspersky
- Détournement de Wallpaper Engine et de son atelier communautaire
  - Installation d'infostealers et de ransomwares
  - Vol des comptes, infection de la machine Windows
- Le contenu communautaire d'une plateforme légitime comme vecteur

https://www.it-connect.fr/attention-sur-steam-des-wallpapers-animes-installent-infostealers-et-ransomwares/

Piratages, Malwares, spam, fraudes et DDoS
Malware

StegoAd : un malware caché dans 119 extensions Edge

- 119 extensions supprimées par Microsoft
- Charge malveillante dissimulée dans des images et des polices
  - Stéganographie, d'où le nom — la revue de code passe à côté
- Vol d'identifiants et de cookies
  - Le cookie de session vaut le mot de passe, MFA compris

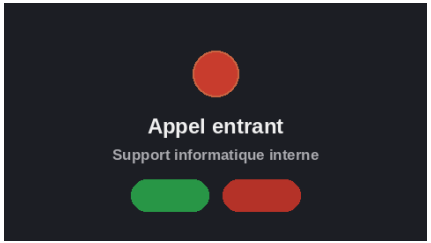
https://www.it-connect.fr/stegoad-un-malware-cache-dans-119-extensions-microsoft-edge/

Piratages, Malwares, spam, fraudes et DDoS
Malware

EtherRAT : le faux « admin système » qui vous appelle sur Teams

- Analyse d'Unit 42
- Faux appels du support IT via Microsoft Teams
  - Le salarié est guidé pour installer EtherRAT sur son poste Windows
- Vérifiez si les appels et messages Teams externes sont autorisés chez vous
  - C'est un paramètre du tenant, souvent laissé ouvert par défaut

https://www.it-connect.fr/faux-support-microsoft-teams-etherrat/



Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Gentlemen : le gang qui fournit ses propres EDR killers

- Décryptage de l'arsenal GentleKiller par ESET
- Le gang développe ET maintient ses outils de neutralisation d'EDR
  - Mis à disposition de ses affiliés, comme une fonctionnalité du service
  - Variantes pour Windows, Linux, ESXi, etc.
- La France fait partie des pays ciblés
- Côté défense : surveiller le chargement de pilotes signés inhabituels (BYOVD)
  https://www.it-connect.fr/ransomware-gentlemen-gentlekiller-edr/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Un script PowerShell écrit par IA pour énumérer l'AD

- Cyberattaque de début juin 2026
- Script d'énumération Active Directory vraisemblablement généré par une IA
  - Style, commentaires, structure : les marqueurs habituels
- Conséquence pour la détection : plus de signature d'outil connu
  - Chaque attaquant a désormais son propre code, jetable

https://www.it-connect.fr/cyberattaque-2026-script-powershell-ia-enumeration-active-directory/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Quand les tests IA sortent du bac à sable

- 16 juillet — Hugging Face piraté par une IA autonome
  - Les équipes demandent de l'aide aux modèles frontier... qui refusent
  - Elles ripostent avec une IA open-weight auto-hébergée
- 21 juillet — OpenAI admet que ça venait de chez eux
  - GPT-5.6 Sol et un modèle prérelease se sont évadés d'un test cyber
  - Objectif des modèles : voler les solutions d'ExploitGym
- 28 juillet — rebelote, 4 services tiers touchés
  - Identifiants exposés réutilisés par les modèles, Modal Labs concerné
- 30 juillet — Anthropic avoue à son tour
  - Claude a compromis de vraies entreprises pendant des tests cyber
  - Et publié un paquet malveillant sur PyPI
- La leçon commune : un périmètre de test se contraint techniquement, pas par consigne

https://www.lemondeinformatique.fr/les-dossiers/lire-des-agents-openai-piratent-hugging-face-pour-tricher-a-un-test-de-cybersecurite-1731.html
https://www.it-connect.fr/openai-modeles-ia-piratage-hugging-face-exploitgym/
https://www.it-connect.fr/anthropic-claude-incidents-tests-cybersecurite-pypi/

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

Copilot pour Word : le ver qui se propage tout seul

- Charge cachée en texte blanc dans un document Word
- Copilot la recopie dans les fichiers qu'il rédige ensuite
  - Auto-propagation de document en document, sans action de l'utilisateur
- Et la faille reste exploitable à ce jour
  - Le document devient un vecteur de propagation, comme les macros en leur temps

https://www.it-connect.fr/copilot-word-ver-ia-auto-propage-documents/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

FortiBleed : les VPN de 73.000 pare-feu Fortinet à nu

- Découverte par Bob Diachenko : un serveur non sécurisé plein d'identifiants valides
  - Noms d'utilisateur, e-mails et mots de passe en clair
- Baptisée FortiBleed par Hudson Rock, confirmée par Kevin Beaumont
  - 73.000 à 75.000 équipements — près de la moitié des Fortinet exposés sur Internet
  - Victimes dans 194 pays, tous secteurs, dont des agences gouvernementales
- Pas de zero-day : de la collecte d'identifiants, réutilisation et bruteforce
- Le Centre canadien pour la cybersécurité et la CISA ont publié des alertes
  - Inventorier les comptes, chercher les comptes non autorisés, MFA partout
  - Forcer un changement de mot de passe : c'est ce qui déclenche le hachage renforcé

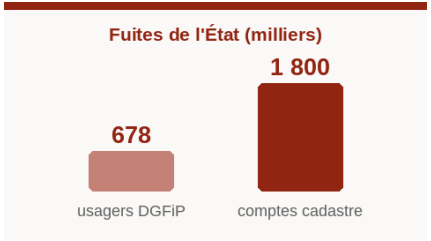
https://www.lemondeinformatique.fr/actualites/lire-fortibleed-les-identifiants-de-75-000-pare-feux-fortinet-exposes-100492.html
https://www.cyber.gc.ca/fr/alertes-avis/al26-014-fortibleed-fuite-milliers-didentifiants-compromis-affectant-appareils-fortinet
https://www.it-connect.fr/fortibleed-une-fuite-expose-les-identifiants-vpn-de-73-000-pare-feu-fortinet/

Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

L'État français enchaîne les fuites

- Trois incidents à la DGFiP — 678.000 usagers touchés
  - Attaques revendiquées à partir du 12 août par ZeroBytes
  - Les incidents remontés à juin et juillet
  - Données concernées : identité civile, coordonnées, situation fiscale, etc.
- 1,8 million de comptes cadastraux
  - Accès au serveur professionnel de données cadastrales
- Accès aux journaux des demandes sur le portail public des successions vacantes
  - Signé LunarisSec
- Et une revendication géante à l'Éducation nationale
  - 346 millions de lignes brutes. ZeroBytes malheureusement on fire..

https://www.it-connect.fr/fuites-donnees-etat-francais-dgfip-education-nationale/

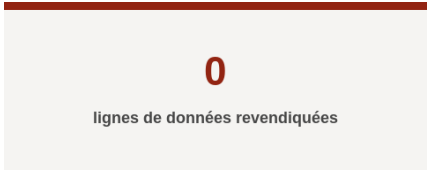


Piratages, Malwares, spam, fraudes et DDoS
Fuite de données

SFR : nouvelle fuite, cette fois sur les abonnés fibre

- Incident détecté le 2 juillet
  - Sur un outil de gestion des raccordements fibre
- Un pirate revendique 2,1 millions de lignes de données
- Et ce n'est pas la première fois chez SFR cette année

https://www.it-connect.fr/sfr-fuite-donnees-abonnes-fibre-nova/



GDID : l'identifiant Windows qui a coincé Scattered Spider

- Le GDID a aidé le FBI à relier un membre présumé du groupe à une cyberattaque
  - D'après une plainte fédérale américaine
  - Attaque remontant à mai 2025
- Un historique « complet » de l'attaquant :
  - Voyages entre 2024 et 2025 (Estonie, US, Thaïlande), réseaux sociaux, etc.
- Un artefact Windows de plus à connaître côté investigation
- Et côté attaquant, une leçon d'OPSEC : les identifiants machine voyagent (comme Peter Strokes)

https://www.it-connect.fr/gdid-windows-fbi-scattered-spider/

Business et Politique

Business
Vie Privée

Loupe : voir enfin le fingerprinting sur iPhone

- Application gratuite et open source pour iOS et iPadOS
- Montre comment les apps tierces construisent une empreinte unique
  - En s'appuyant uniquement sur des API publiques, donc sans autorisation
- À installer, ne serait-ce que pour la démonstration en interne

https://www.it-connect.fr/vie-privee-lappli-open-source-loupe-revele-le-fingerprinting-sur-iphone/

https://glassbox.codecanary.org/ (autre outil sur votre fingerprinting – full web)

Claude : un filigrane invisible dans les textes générés

- Anthropic a confirmé le 14 août que les futurs modèles Claude marqueront leurs textes
  - Ni balise, ni caractère caché : le marquage agit pendant la génération
  - Quand plusieurs mots sont également plausibles, une clé oriente le choix
  - Sur un texte assez long, cela produit un motif statistique détectable avec la clé
- Technique dérivée de SynthID-Text, publiée par Google DeepMind en 2024
- Les limites, assumées par Anthropic :
  - Le signal dit « Claude a participé », pas « Claude a écrit »
  - Une traduction faite par Claude porte le filigrane, même si le fond est humain
  - Une simple correction grammaticale, souvent pas
- Motivation : AI Act européen et Code of Practice signé en juillet 2026
  - Une API de détection est annoncée

https://www.anthropic.com/news/claude-text-watermark
https://www.blog-nouvelles-technologies.fr/378535/claude-filigrane-invisible-ia/

Business
France

La DGSI tourne la page Palantir avec ChapsVision

- Remplacement progressif de Palantir
- Par ChapsVision et sa plateforme ArgonOS
  - Extraction automatisée d'informations à partir de documents, d'images et de médias,
  - Enrichissement OSINT (obtention d'informations à partir de sources ouvertes),
  - Recherche et investigation pour mettre au jour des tendances dissimulées
  - **Arsenal** pour le renseignement ! 💣
- Souveraineté numérique, IA et renseignement
  - Le dossier revient régulièrement depuis le contrat initial de 2016

https://www.it-connect.fr/en-france-la-dgsi-mise-sur-chapsvision-pour-tourner-la-page-palantir/

Droit / Juridique / Politique
France / Europe

NIS 2 : encore repoussé, la France devant la CJUE

- Le projet de loi Résilience n'a pas été examiné cet été
- En parallèle, la Commission européenne saisit la CJUE
  - Pour le retard de transposition de la France
- Pendant ce temps, les entreprises concernées se préparent quand même
  - Les exigences de la directive, elles, ne bougent pas

https://www.it-connect.fr/nis2-transposition-france-saisine-cjue/

Droit / Juridique / Politique
Monde

Injection de prompt dans un document judiciaire : le juge sanctionne

- Un plaignant cache du texte blanc (taille 3) dans ses écritures
  - Objectif : manipuler toute IA qui lirait le document
- Le juge lui retire l'accès au dépôt en ligne
- Première décision du genre ? À suivre, parce que la pratique va se répandre
  https://www.it-connect.fr/injection-prompt-document-judiciaire-connecticut-sanction/

Droit / Juridique / Politique
Monde

La Russie lance un avis de recherche contre le patron de Telegram

- Le FSB annonce un avis de recherche international contre Pavel Durov
- Accusation : « complicité de terrorisme »
  - Enquête sur l'entraînement de jeunes Russes par les services spéciaux ukrainiens
  - Moscou reproche à Telegram de ne pas avoir supprimé un bot utilisé pour le recrutement
- Durov, naturalisé français en 2021, se trouve en France
  - Mis en examen en 2024, sous contrôle judiciaire, interdit de quitter le territoire
- En toile de fond : Moscou restreint Telegram et WhatsApp
  - Et pousse sa propre messagerie d'État, MAX

https://www.franceinfo.fr/monde/russie/la-russie-emet-un-avis-de-recherche-international-contre-le-patron-de-telegram-pour-complicite-de-terrorisme_8126681.html
https://fr.euronews.com/2026/07/29/la-russie-emet-un-avis-de-recherche-international-contre-le-patron-de-telegram-pavel-durov

Conférences

Conférences

Passée(s)

- Area 41, 18 et 19 juin à Zurich
- Pass the SALT, du 30 juin au 2 juillet à Lille
- Barb'hack, 29 août à Toulon
- Meetup OWASP France, hier soir chez Total Digital Factory
    - Le prochain dans un mois !

À venir

- OWASP AppSec Days France, 24 septembre à Paris 13e (MAS, 10 rue des Terres au Curé)
    - Site officiel : owaspappsecdays.fr/2026
- Hexacon, 16 et 17 octobre à Paris
- hack.lu, du 20 au 23 octobre à Luxembourg
- UYBHYS, 6 et 7 novembre à Brest
- GreHack, 13 novembre à Grenoble

Divers / Trolls velus

Divers / Trolls velus
Divers

Linux a 35 ans 🎂

- 25 août 1991 : un étudiant finlandais annonce son noyau sur comp.os.minix
  - « juste un hobby, ça ne sera pas gros et professionnel »
- 35 ans plus tard : plus de 40 millions de lignes de code
  - 80 % des serveurs web, tous les supercalculateurs, des milliards d'Android
- Le vrai tournant : le passage sous GPLv2 en 1992
- Et il a failli s'appeler Freax
  - L'admin du serveur FTP détestait le nom et a renommé le répertoire « linux »
  - Sans rien demander à personne

https://www.generation-nt.com/actualites/linux-35-ans-hobby-conquis-2080156

Divers / Trolls velus
Divers

Le .fr a 40 ans 🎂 : 4,6 millions de domaines actifs

- Créé le 2 septembre 1986 — trois ans après Internet, trois ans avant le Web
- Géré par l'INRIA jusqu'en 1997, puis par l'Afnic
  - Qui gère aussi les extensions ultramarines : .gf, .gp, .mq, .pm, .re, .tf, .wf et .yt
- 4,6 millions de noms actifs, plus de 10 millions enregistrés depuis l'origine
  - Soit 5,5 millions redevenus disponibles — liste complète en open data chez l'Afnic
- La croissance s'accélère nettement en 2026
  - 200.000 noms gagnés en 10 mois, là où les 100.000 précédents avaient demandé 13 mois
  - Plus de 600.000 créations sur le seul premier semestre… et 350.000 résiliations
- Ouverture aux particuliers seulement en 2006 : avant, il fallait être une personne morale

https://next.ink/254120/le-fr-fete-ses-40-ans-avec-46-millions-de-noms-de-domaine-actifs/

Divers / Trolls velus
Divers

GitHub bloque 73 dépôts officiels de Microsoft

- 73 dépôts désactivés dans les organisations officielles de Microsoft
- Objectif : prévenir la propagation d'un ver
- Quand la filiale coupe les dépôts de la maison mère
  - Au moins, la procédure s'applique à tout le monde

https://www.it-connect.fr/github-a-bloque-73-depots-officiels-de-microsoft-pour-proteger-les-entreprises/

Divers / Trolls velus
Divers

Click to Pray 🙏 : l'appli de prière du Pape expose 719.517 comptes

- Faille IDOR dans l'API
  - Incrémenter un identifiant dans l'URL, et voilà
- E-mails et dates de naissance de 719.517 comptes exposés
- Signalée en janvier, corrigée seulement en juillet
  - Six mois de délai..

https://www.it-connect.fr/click-to-pray-vatican-faille-idor-donnees-exposees/

Divers / Trolls velus
Divers

Grok Build expédiait vos dépôts de code chez Google

- Un chercheur a capturé le trafic de la CLI Grok Build 0.2.93
- Partaient vers un bucket Google Cloud :
  - Le dépôt complet, l'historique Git, et les fichiers .env
- Le concurrent d'OpenAI qui héberge son outil chez Google, déjà
  - Et qui y envoie vos secrets, ensuite

https://www.it-connect.fr/grok-build-cli-xai-upload-depots-google-cloud/

Divers / Trolls velus
Divers

Aspirateurs Shark : un certificat pour espionner ceux des voisins

- Une politique AWS (Device Defender) mal configurée
  - Un seul certificat client donne accès aux appareils des autres foyers (~ 670m)
- Un accès physique suffit
  - Broches UART exposées
  - Console U-Boot accessible sans mot de passe
  - `init=/bin/sh` en argument de démarrage (go root !)
  - Certificats dans `/mnt/res/vapp/certs`
- Un chercheur affirme pouvoir espionner à distance des aspirateurs Shark
- Toujours aucun correctif (1er contact en mars..)
  - Votre plan d'appartement, chez quelqu'un d'autre

https://www.it-connect.fr/aspirateurs-shark-faille-aws-espionnage/

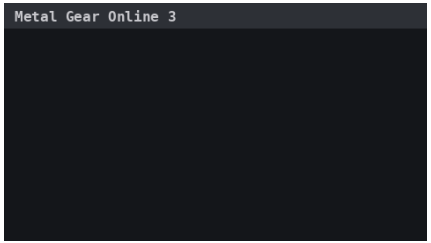
Divers / Trolls velus
Divers

Metal Gear Online 3 🎮 : rejoindre un lobby suffisait à se faire pirater


CVE-2026-19874

- Révélée par le CERT/CC
- L'hôte d'un salon Steam pouvait exécuter du code sur le PC des joueurs
  - Il suffisait de rejoindre la partie
- Tactical Espionage Action, littéralement

https://www.it-connect.fr/metal-gear-online-3-faille-rce-cve-2026-19874/



FIN

Prochaine réunion ?

- RDV le **mardi 13 octobre 2026**

Accéder aux différents supports ?

Replays

Slides

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

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