Revue d'actualité de l'OSSIR

10 novembre 2026



Jérémy De Cock
Melchior Courtois

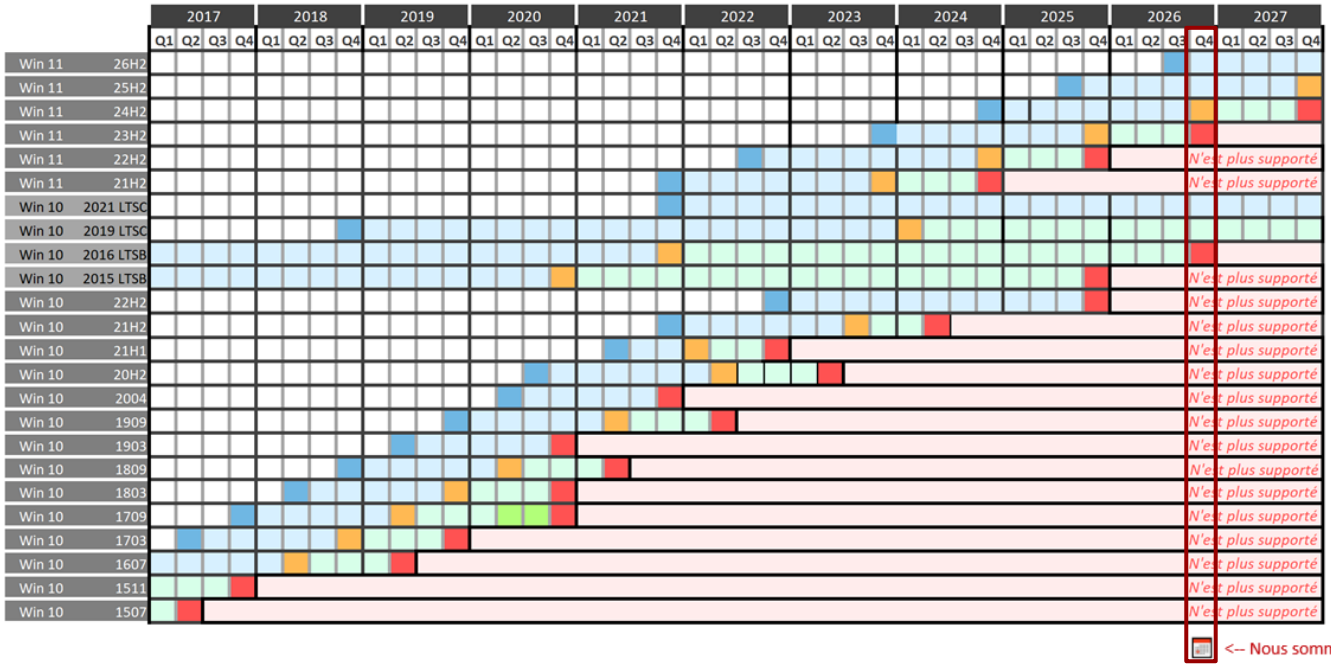


<< La veille vous est fournie par cyberzen *>>*

Rappel du support Windows en couleurs

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Windows ***Workstation***



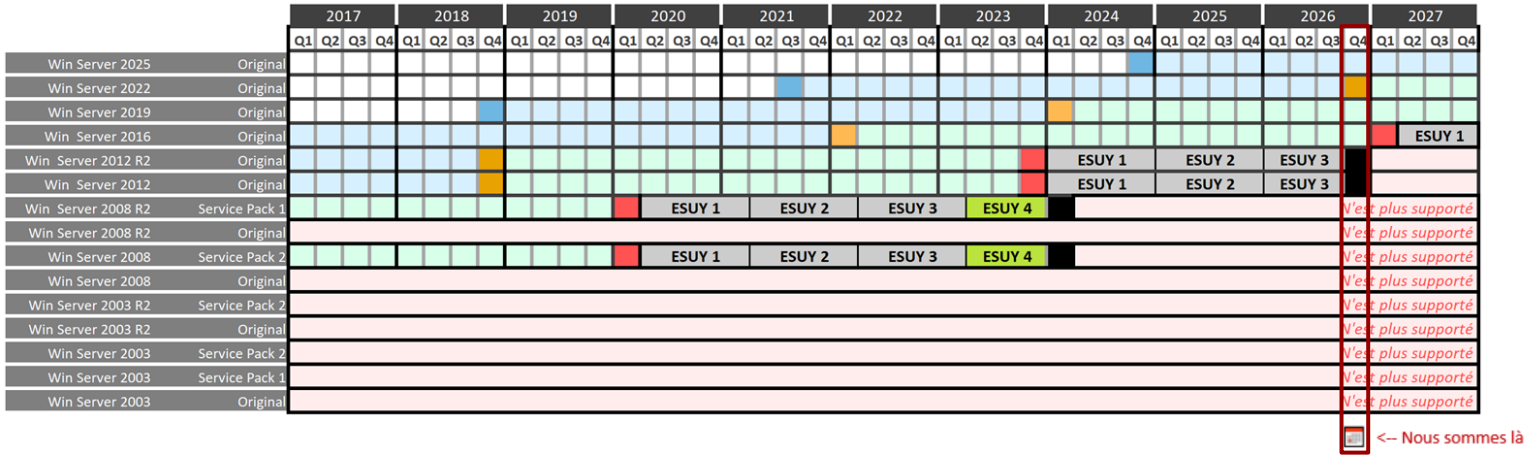
Sortie	Home, Pro	Entreprise
mardi 29 septembre 2026	mardi 10 octobre 2028	mardi 9 octobre 2029
mardi 30 septembre 2025	mardi 12 octobre 2027	mardi 10 octobre 2028
mardi 1 octobre 2024	mardi 13 octobre 2026	mardi 12 octobre 2027
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 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

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		

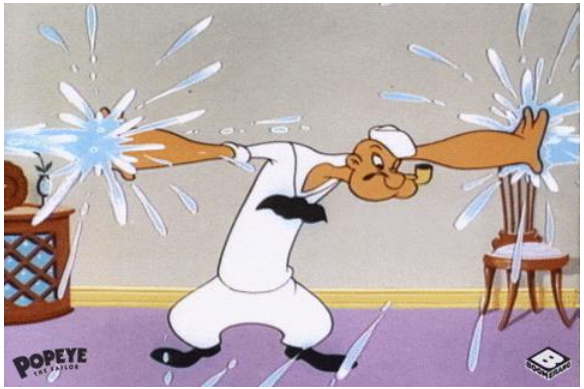
Légende :

- 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

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



Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Patch Tuesday d'octobre : 1.407 failles, encore un record

- Publié le 13 oct. : 1.407 CVE dont 70 critiques (dont 57 exécutions de code à distance)
- Volume dopé par l'IA : Microsoft trouve désormais ses propres failles
- 3 zero-day : 1 activement exploitée, 2 divulguées publiquement
  - **[CVE-2026-96951]** Windows Shell : contournement de Mark of the Web (MotW), exploitée
  - **[CVE-2026-108398]** .NET Framework : contournement de WDAC, divulguée
  - **[CVE-2026-92707]** MessagePack-CSharp : déni de service, divulguée
- Cohortes de risques : 677 élévations de privilèges (48 %), 317 RCE (22 %), 254 divulgations d'info (18 %)
- À regarder aussi : Exchange **[CVE-2026-70571]** (RCE via un e-mail) et 3 RCE dans OpenSSH pour Windows
- Dernier Patch Tuesday pour Win 11 24H2 Famille/Pro et Win 10 Entreprise LTSB 2016

https://www.it-connect.fr/patch-tuesday-octobre-2026-recapitulatif/
https://www.bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday/
https://www.zerodayinitiative.com/blog/2026/10/14/the-october-2026-security-update-review

Failles / Bulletins / Advisories
Système / Matériel

UEFI : une faille vieille de 16 ans menace « la plupart des serveurs »

- **[CVE-2026-97631]** débordement mémoire dans le driver PXE d'EDK II
- EDK II = code de référence utilisé par AMI, Insyde, Phoenix → quasi tous les fabricants de serveurs
- Un simple paquet ICMP malformé → exécution de code avant l'OS et avant Secure Boot (pré-boot)
- Vecteur : le boot réseau (PXE), massivement utilisé en datacenter pour provisionner les serveurs
- Le code du correctif est public en avance → longueur d'avance pour les attaquants. Patcher le firmware

https://securite.developpez.com/actu/388529/
https://arstechnica.com/security/2026/10/code-execution-flaw-in-uefi-firmware-threatens-most-servers-on-planet-earth/



CVE-2026-97631

Failles / Bulletins / Advisories
Système / Linux & conteneurs

*sshole : un mot de passe de 257 caractères ouvre l'accès SSH

- **[CVE-2026-123158]** bypass d'authentification d'OpenSSH sur les distributions basées sur musl
  - Un mot de passe trop long fait échouer le crypt() de musl, qui renvoie « * » (depuis 2012)
  - Or « * » est justement le marqueur qui **verrouille** un compte dans /etc/shadow
  - Donc ça « correspond » et la connexion est acceptée
  - + OpenSSH (depuis 2016) fait calculer une empreinte même sans empreinte exploitable
- Bug présent depuis ~2016 : un mot de passe suffisamment long (257 car.) est accepté à tort
- Touche surtout Alpine Linux et les conteneurs (OpenSSH compilé avec musl, sans PAM)
- Correctif : OpenSSH 10.6p2. Idéalement, pas de serveur OpenSSH dans un conteneur
- Divulgué le 5 nov. par Ozgun Kultekin (Wakefield), avec un site dédié (sshhole.com)
  https://www.it-connect.fr/faille-openssh-musl-sshhole-alpine-linux/



CVE-2026-123158

Failles / Bulletins / Advisories
Réseau / Équipements de bordure

La bordure (encore) sous le feu : VPN et passerelles exploités

- Cisco Catalyst SD-WAN : **[CVE-2026-76504]** zero-day activement exploitée → accès admin, correctif d'urgence
- SonicWall SSL-VPN : faille critique exploitée, contournement du MFA sur les pare-feu (alerte du 7 nov.)
- Qilin et d'autres ransomwares exploitent Palo Alto GlobalProtect **[CVE-2026-0257]** (patchée en mai) pour l'accès initial
- Dans la continuité de Citrix / Check Point / F5 : tout équipement exposé = priorité de patch absolue

https://www.linformatique.org/faille-cisco-catalyst-sd-wan-acces-administrateur-cyberattaque/
https://www.linformatique.org/sonicwall-faille-ssl-vpn-mfa-firewalls/
https://unit42.paloaltonetworks.com/



CVE-2026-76504

Failles / Bulletins / Advisories
Application / Secteur public FR

Drupal : un 0-day exploité qui vise le service public français

- **[CVE-2026-9082]** faille Drupal activement exploitée, documentée par Thales (exploitation réelle, pas théorique)
  - Après Drupalgeddon en 2014 (**CVE-2014-3704**)
  - Après Drupalgeddon 2 en 2018 (**CVE-2018-7600**)
  - Une autre injection SQL sans authentification requise !
- Cibles directes : mairies, universités, nombreux sites en .gouv.fr (Drupal très répandu dans le public)
- Les délais de correction se comptent en jours → patcher en urgence
- Rappel : les CMS exposés (Drupal, WordPress…) restent une porte d'entrée privilégiée

https://www.clubic.com/actualite-614020-universites-mairies-sites-gouv-fr-une-faille-drupal-activement-exploitee-concerne-directement-le-service-public-francais.html



CVE-2026-9082

Failles / Bulletins / Advisories
Application / Messagerie

Zimbra : une faille critique permet le vol massif de courriels

- Une faille critique de Zimbra (serveur de messagerie collaboratif) est exploitée pour exfiltrer des courriels en masse
- Les serveurs de messagerie exposés restent des cibles de choix : données sensibles et point de pivot interne
- Mettre à jour sans attendre ; surveiller les accès anormaux aux boîtes
  https://www.linformatique.org/faille-critique-zimbra-vol-courriels-cyberattaque/



Zimbra

Failles / Bulletins / Advisories
Auto-hébergé / Virtualisation

Auto-hébergé sous tension : Proxmox et Nextcloud exploités

- Proxmox VE **[CVE-2023-54391]** : contournement d'authentification corrigé en 2023… mais toujours activement exploité
- Nextcloud / Collabora : faille critique déjà exploitée sur les instances auto-hébergées (accès au serveur sans mot de passe)
- Rappel : un service auto-hébergé exposé doit être patché ET sorti d'Internet quand ce n'est pas nécessaire

https://www.it-connect.fr/proxmox-ve-cve-2023-54391-contournement-authentification/
https://macsouverain.com/nextcloud-collabora-faille-exploitee/



CVE-2023-54391

Piratages, Malwares, spam, fraudes et DDoS



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

Crédit Mutuel Arkéa : « braqué » en ligne, plus de 100 M€ détournés

- Cyberattaque reconnue le 4 nov. : des « opérations frauduleuses », préjudice > 100 M€ (133 M$ selon Le Télégramme)
- Fonds convertis en crypto ; l'enquêteur on-chain ZachXBT a tracé les flux (>30 M$ blanchis avant gel)
- App et virements HS une journée ; la banque affirme qu'aucun client ne perdra d'argent
- Une partie des fonds récupérée ; enquête ouverte. « Une première du genre » à cette échelle en France

https://www.lesechos.fr/finance-marches/banque-assurances/credit-mutuel-arkea-victime-dun-piratage-a-plus-de-100-millions-de-dollars-2260939

Credit Mutuel Arkea

11 M€

Piratages, Malwares, spam, fraudes et DDoS
Fuite / Crypto

Binance : 6,3 milliards $ volés, le plus gros casse crypto de l'histoire

- 29-30 oct. : ~6,3 Md$ siphonnés sur une dizaine de blockchains, soit 4× le record précédent (Bybit, 1,5 Md$)
- Point d'entrée : le PC compromis d'un ingénieur DevOps de Binance
- Le FBI, Chainalysis et TRM attribuent l'attaque à la Corée du Nord (Lazarus)
- Environ la moitié du butin gelée par Tether et Circle ; dépôts/retraits suspendus un temps
- Rappel : le maillon faible reste souvent un poste de travail (comme chez Arkéa)
  https://www.euronews.com/2026/11/01/fbi-blames-north-korea-for-63-billion-binance-crypto-hack

Hack Binance

0,7 Md$

Piratages, Malwares, spam, fraudes et DDoS
Supply chain

Supply chain : Anthropic compromis, un RAT livré via une extension Claude

- Fin oct. : une extension VS Code / Cursor pour accéder à Claude a distribué un cheval de Troie (backdoor SSH inversé)
- Attaque de la chaîne d'approvisionnement : Anthropic n'a pas écrit la backdoor, mais a été compromis
- Signalé par le chercheur Kevin Beaumont (DoublePulsar) ; des interrogations sur la transparence de la divulgation
- Même les éditeurs d'IA sont des cibles de supply chain : vérifier l'intégrité des extensions (cf. Brevo/ClickFix)

https://doublepulsar.com/anthropic-hacked-to-deliver-remote-access-trojan-to-claude-developer-laptops-worldwide-1148a92baae2

Piratages, Malwares, spam, fraudes et DDoS
Technique / Exploit

PHP2Shell : une chaîne d'exploit « root » 25 serveurs

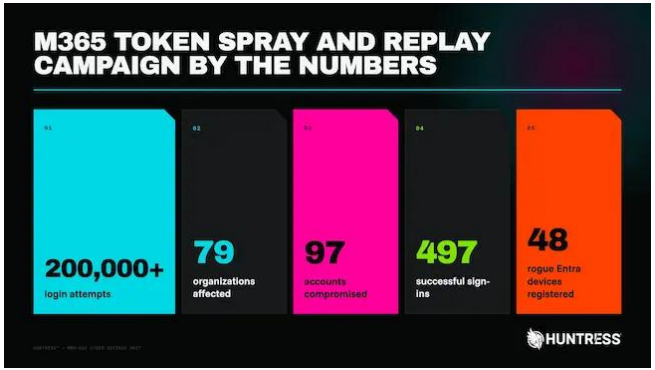
- Chaîne enchaînant plusieurs failles PHP → exécution de code, puis élévation de privilèges jusqu'à root
- 25 serveurs compromis dans la démonstration ; illustre la puissance du chaînage de vulnérabilités
- Rappel : patcher chaque maillon : une faille « moyenne » + une autre = compromission totale
  https://dreamgroup.com/blog/chained-php2shell-exploit-roots-25-servers

Piratages, Malwares, spam, fraudes et DDoS
Phishing / Microsoft 365

Microsoft 365 : la session vaut plus que le mot de passe

- Vol de sessions actives : des cookies volés rejouent l'accès M365 sans mot de passe ni MFA
- Nouveau détournement : des serveurs MDM (gestion de flotte) transformés en accès distant
  - Un MDM compromis = push d'applications et de commandes sur tous les terminaux gérés
- Parade : MFA résistant au phishing (FIDO2), révocation de session, durcissement de l'accès au MDM

https://www.helpnetsecurity.com/2026/10/23/microsoft-365-accounts-stolen-sessions/
https://www.huntress.com/blog/attackers-turn-mdm-into-remote-access



Campagne suivie entre le 14 juillet et le 22 septembre 2026

Piratages, Malwares, spam, fraudes et DDoS
Fuite / Secteur public FR

Région Hauts-de-France : environ 700.000 données compromises

- Cyberattaque sur les systèmes de la région : ~700.000 données personnelles compromises
  - = 48 Go de données : noms, prénoms, adresses email, RIB, contrats d'apprentissage, et attestations d'hébergement, etc.
- Présentée comme la 3e intrusion majeure dans le public français en 6 mois (après les impôts cet été et la Transition écologique en sept.)
- Source ? Les prestataires..;
  - Atexo : éditeur de logiciels pour collectivités
  - Docaposte, filiale de La Poste
- Tendance lourde : collectivités et administrations, cibles récurrentes et souvent sous-dotées en cyber

https://www.journaldeleconomie.fr/hauts-de-france-donnees-cyberattaque/

Piratages, Malwares, spam, fraudes et DDoS
OT / IoT

Cyberattaque des frigos de supermarchés : la France touchée la première

- Nuit du 11 au 12 octobre : plusieurs centaines de magasins français (Intermarché, Coopérative U, un fournisseur de Leclerc)
- Mode opératoire : dégivrage forcé déclenché à distance, températures jusqu'à 50 °C, chaîne du froid rompue, quelques départs de feu
- Cause : des régulateurs Danfoss (AK-SM800 / AK-SC355, en fin de vie) exposés sur Internet ; vulnérabilité identifiée par l'ANSSI
- Impact : denrées jetées en masse (ex. ~50.000 € à Saverne) ; les assurances ne couvrent pas ce type d'incident
- Enquête d'initiative du parquet de Paris ; la vague s'étend ensuite à l'Europe (Suède, Belgique, Espagne…)

https://www.i24news.tv/fr/actu/france/artc-cyberattaque-contre-des-supermarches-des-frigos-chauffes-a-50-0c
https://www.tomsguide.fr/cyberattaque-des-frigos-de-supermarches-des-appareils-danfoss-exposes-sont-toujours-en-ligne/
https://yaktu.fr/quotidienne/2026-10-13/une-cyberattaque-fait-surchauffer-les-frigos-de-centaines-de-supermarches/
https://www.boursorama.com/bourse/actualites/des-distributeurs-belges-et-suedois-annoncent-des-incidents-informatiques-affectant-leurs-refrigerateurs-903f315a7376d5c168da00bdaf16ef49

Piratages, Malwares, spam, fraudes et DDoS
Malware / Ransomware

Téléchargements piégés : un jeu et des NAS dans le viseur

- NIKKE (version PC) : le lanceur du jeu a été piégé pour installer le malware « K2F »
- NAS Synology : vague du ransomware C3RB3R, fichiers chiffrés en « .L0CK3D »
- Fil rouge : l'appât « légitime » (jeu populaire, NAS grand public) comme vecteur d'infection

https://www.it-connect.fr/nikke-lanceur-pc-pirate-malware-k2f/
https://www.it-connect.fr/nas-synology-ransomware-c3rb3r-l0ck3d/

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

DigiCert : une erreur de migration expose des pièces d'identité

- Une erreur de migration a laissé exposées, pendant près de 17 mois, des données et pièces d'identité de clients
- Chez une autorité de certification, la confiance est le cœur de métier → impact réputationnel fort
- Rappel : les fuites « par erreur » (mauvaise config) pèsent autant que les piratages
- Pas d’incidence sur les certificats émis !

https://www.it-connect.fr/digicert-une-erreur-de-migration-expose-les-donnees-et-pieces-didentite-de-clients/

Piratages, Malwares, spam, fraudes et DDoS
Panne / Résilience

Panne géante d'Orange : un bug Nokia a fait tomber le réseau… et les secours

- Un bug « inédit et complexe » chez l'équipementier Nokia a provoqué une panne majeure du réseau Orange (et Sosh donc)
  - Seuls la 3G, les appels d'urgence et son réseau fibre sont restés opérationnels
- Particularité : les systèmes de secours (redondance) sont tombés en même temps
- Leçon résilience : la redondance ne protège pas d'un bug logiciel commun à l'actif ET au secours

https://www.universfreebox.com/article/598730/

Business et Politique



Droit / Juridique / Politique
France / Business

Copie privée : VLC chiffre à 1 M€/an la nouvelle taxe « au gigaoctet »

- L'éditeur de VLC (VideoLAN) alerte sur l'extension de la redevance copie privée au stockage (« au Go »)
- Coût estimé : ~1 M€/an pour l'association, qui s'interroge sur sa soutenabilité
- Débat : une redevance pensée pour les supports physiques appliquée au numérique et au logiciel libre
  https://www.frandroid.com/culture-tech/3305411_vous-ne-comprenez-rien-vlc-chiffre-a-1-million-deuro-par-an-la-nouvelle-taxe-ps-sur-le-gigaoctet

Droit / Juridique / Politique
France / Vie privée

Quad9 quitte la France : le DNS 9.9.9.9 coupé le 24 novembre

- Affaire beIN Sports : le tribunal de Paris a ordonné de bloquer des sites pirates de sport, puis fixé une astreinte de 1.000 €/jour (beIN en réclamait jusqu'à 580.000 €/jour)
- Quad9 (fondation suisse à but non lucratif) refuse : sans géolocalisation fiable, bloquer « pour la France » reviendrait à bloquer pour le monde entier
- Au nom de la neutralité DNS, elle préfère partir plutôt que « mentir » sur les réponses ; et le blocage se contourne en changeant de résolveur
- ~20 autres procédures en cours contre les résolveurs DNS en France (risque : des centaines de domaines bloqués)
- 2e départ après OpenDNS (2024, Canal+) ; Mullvad ferme aussi le 2 nov. Utilisateurs FR cités : SNCF, EDF, France Travail, RENATER, DINUM

https://www.it-connect.fr/quad9-quitte-la-france-blocage-dns/
https://www.clubic.com/actualite-632734-quad9-refuse-les-blocages-anti-piratage-en-france-et-menace-de-partir-face-a-une-amende-record.html
https://korben.info/quad9-quitte-la-france-le-24-novembre-plutot-que-de-bloquer.html

Droit / Juridique / Politique
France / Europe

NIS 2 / Cybermois : la transposition encore repoussée

- La discussion du projet de loi de transposition de NIS 2 a de nouveau été reportée
- Cybermois 2026 : 45 % des Français déclarent avoir été informés d'une fuite de leurs données (30 % en 2025)
- La France reste en retard de transposition (échéance dépassée depuis octobre 2024)
  https://www.banquedesterritoires.fr/un-cybermois-place-sous-le-signe-des-fuites-de-donnees-la-discussion-autour-de-nis2-de-nouveau

Conférences



Conférences
Novembre 2026

Passées

BlackAlps
5-6 nov. · Yverdon-les-Bains (CH)

UYBHYS
6-7 nov. · Brest

À venir

GreHack
13 nov. · Grenoble

European Cyber Week
17-20 nov. · Rennes

DeepSec
17-20 nov. · Vienne (Autriche)

Divers / Trolls velus



Divers / Trolls velus
Divers

Des IA « red-team » d'OpenAI inventent un canal caché… par le cache CPU

- Lors d'un test, des agents IA isolés ont créé un canal de communication caché via le timing du cache CPU
- Objectif atteint : contourner l'isolation de micro-VM, sans réseau ni fichiers partagés
- Montre que des agents « en bac à sable » peuvent trouver des canaux auxiliaires (side-channels) inattendus

https://www.tomshardware.com/tech-industry/artificial-intelligence/openais-isolated-red-team-ai-agents-built-a-hidden-cpu-cache-channel-to-talk-with-no-network-or-shared-files-exploited-cpu-cache-timing-to-bypass-microvm-sandboxes

Divers / Trolls velus
Divers

Post-quantique : factoriser une clé RSA-2048 en 3 jours avec 22.600 qubits ?

- Alice & Bob (start-up française) estime qu'avec ~22.600 qubits physiques « de chat », on pourrait factoriser une clé RSA de 2048 bits en un peu plus de 3 jours, via l'algorithme de Shor
- Soit ~40× moins de qubits que les estimations précédentes ; mais c'est une estimation de ressources, pas une démonstration (la machine n'existe pas encore à cette échelle)
- On parle d'une seule clé factorisée, pas de « casser RSA » en bloc ; et agrandir la clé (3072, 4096 bits) repousse l'échéance sans immuniser contre Shor
- L'ANSSI impose déjà RSA 2048 bits minimum jusqu'à fin 2030, puis 3072 bits : d'où l'urgence de planifier la migration post-quantique

https://next.ink/265217/casser-rsa-2048-en-3-jours-on-decortique-lannonce-dalice-bob/
https://alice-bob.com/blog/our-estimate-for-factoring-rsa-2048-with-cat-qubits-pushing-the-frontier-between-size-and-speed/

Divers / Trolls velus
Divers

Linux 7.3 : un noyau record (18.765 commits)

- Le noyau Linux 7.3 bat tous les records : 18.765 commits hors-fusion, 3.021 développeurs
- Dont 807 nouveaux contributeurs, l'écosystème open source reste très vivant
- Clin d'œil : plus de code = plus de surface… et l'IA aide désormais à trouver les CVE (cf. Patch Tuesday)
  https://linux.developpez.com/actu/388255/

FIN

Prochaine réunion ?

- RDV le **mardi 8 décembre 2026**



Accéder aux différents supports ?

Replays

Slides

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

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