Revue d'actualité de l'OSSIR

10 février 2026

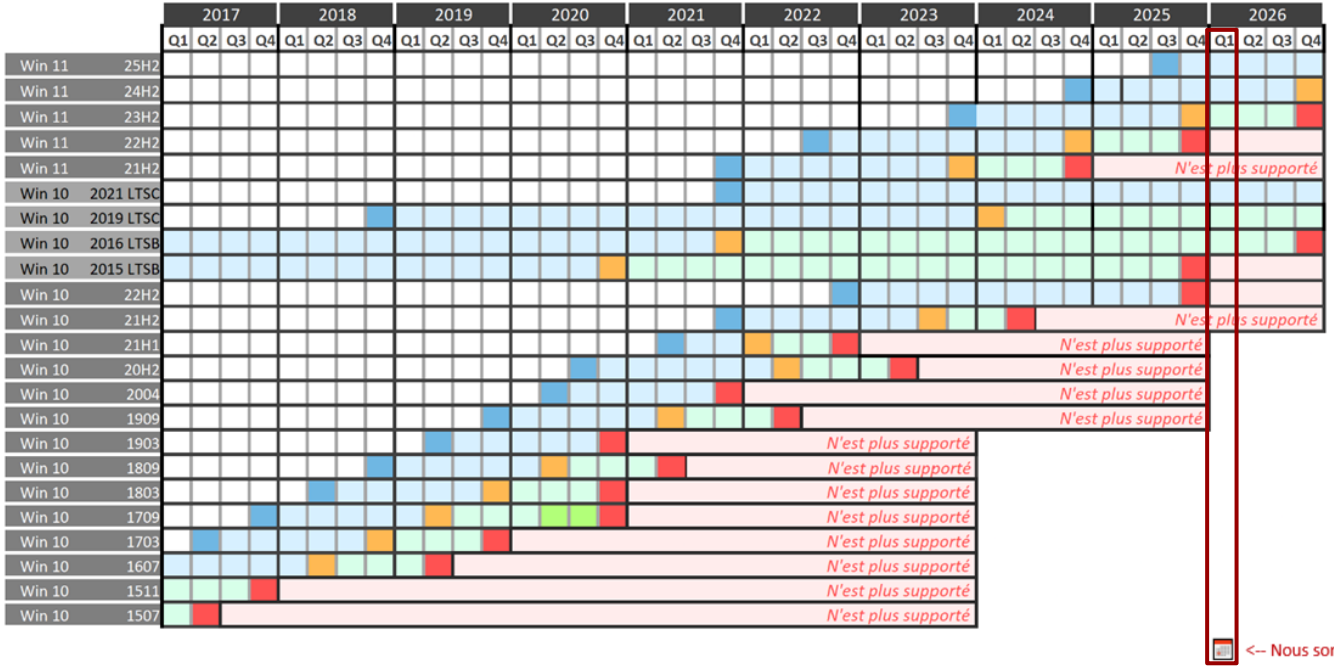
Jérémy De Cock
Melchior Courtois

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

Rappel du support Windows en couleurs

Failles / Bulletins / Advisories (MMSBGA)

Microsoft - Windows ***Workstation***



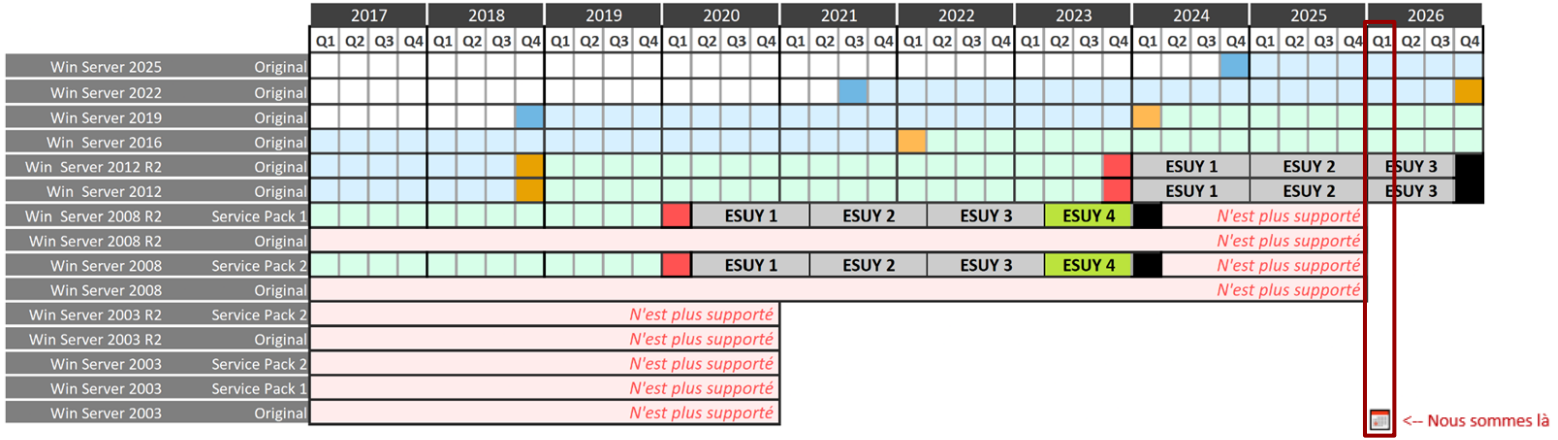
Sortie	Home, Pro	Entreprise
mardi 30 septembre 2025	mardi 12 octobre 2027	mardi 10 octobre 2028
mardi 1 octobre 2024	mardi 13 octobre 2026	mardi 12 octobre 2027
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi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



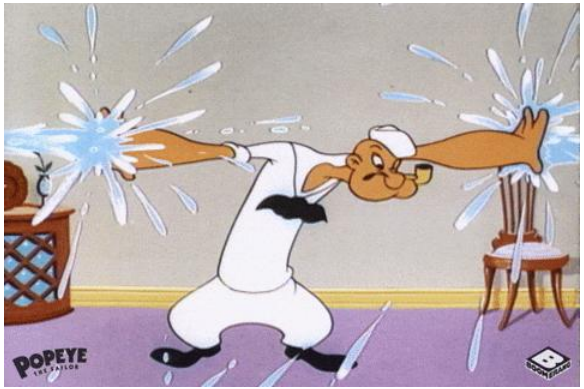
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre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

Bulletin de janvier, 114 vulnérabilités patchées dont

- 3 vulnérabilités de type 0-day :
  - [**CVE-2026-20805**] Leak mémoire, Desktop Window Manager
    - Ajoutée au catalogue KEV de la CISA
    - Affecte Windows 10 et 11 & Windows Server 2012 à 2025
  - [**CVE-2026-21265**] Bypass, Secure Boot
    - Cf. https://www.ossir.org/paris/supports/2025/2025-10-14/2025-10-14.pdf
    - Les premiers certificats expirent en juin 2026 !
  - [**CVE-2023-31096**] Élévation de privilèges, Pilote Agere Modem
    - Documentée en 2023 par le MITRE
      - Deux nouveaux pilotes natifs supprimés : `agrsm64.sys` et `agrsm.sys`
    - Affecte Windows 10 et 11 & Windows Server 2008 à 2025
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2026-20822**] Élévation de privilèges, Microsoft Graphics Component
  - [**CVE-2026-20854**] RCE, LSASS
  - [**CVE-2026-20876**] Élévation de privilèges, VBS
  - [**CVE-2026-20952,20953**] RCE, Microsoft Office
  - [**CVE-2026-20957**] RCE, Microsoft Excel
  - [**CVE-2026-20944**] RCE, Microsoft Word

https://www.it-connect.fr/patch-tuesday-janvier-2026-recapitulatif/

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

Le choix de Kubernetes

- Problème de sécurité présent dans la fonction RBAC
  - Au niveau de la permission nodes/proxy GET : droit en lecture accordé pour la surveillance et l'observabilité
- Vérification des droits lors de la connexion mais pas de vérification lors de l'envoi de commande ultérieur → possible d'exécuter des commandes sur n'importe quel Pod du cluster Kubernetes
- Pas de patch prévu (ni CVE) par Kubernetes car pas de vulnérabilité selon eux
  - `« Après un examen approfondi avec SIG-Auth et SIG-Node, nous confirmons notre décision selon laquelle ce comportement fonctionne comme prévu et ne fera pas l'objet d'un CVE »`
- Script de détection mise en ligne par le chercheur ayant détecté la faille :
  - https://gist.github.com/grahamhelton/f5c8ce265161990b0847ac05a74e466a

https://www.it-connect.fr/kubernetes-cette-vulnerabilite-permet-une-execution-de-code-a-distance-mais-elle-ne-sera-pas-patchee/

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

4 vulnérabilités sur GLPI

CVE-2026-23624
CVE-2026-22247
CVE-2026-22248
CVE-2026-22044

- Affectent soit GLPI 10 soit GLPI 11 soit les deux :
  - CVE-2026-23624 - Vol de session
  - CVE-2026-22248 - RCE via chargement d'un fichier malveillant
  - CVE-2026-22247 - SSRF via un détournement de la fonction de Webhooks
    - Inaccessibles depuis l'extérieur
  - CVE-2026-22044 - Injection SQL à partir d'un utilisateur authentifié
- Bien pensé à patcher

https://www.it-connect.fr/glpi-11-0-5-et-glpi-10-0-23-deux-mises-a-jour-de-securite-a-appliquer-maintenant/

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

N8n, une vulnérabilité critique de plus


CVE-2026-25049

- Possible d'exécuter des commandes système sur l'hôte exécutant n8n
  - Prérequis : utilisateur authentifié avec droits de création et modification de workflow
- Peut entraîner une exfiltration de données, vol d'identifiants et déploiement de backdoor
- Patch disponible : v1.123.17 ou v2.5.2

https://www.it-connect.fr/n8n-cve-2026-25049-execution-code-a-distance/

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

2 CVE mises en lumière chez Ivanti

CVE-2026-1281
CVE-2026-1340

- Concernent la solution Ivanti Endpoint Manager Mobile (EPMM)
  - Plate-forme de gestion de la mobilité d'entreprise (MDM/UEM)
  - 2 RCE unauthenticated
- Pas de correctif permanent
  - Patch disponible à appliquer à chaque mise à jour ou modification du système
  - Correctif prévu pour S1 2026
- POC et résultat des tests en lien

https://labs.watchtowr.com/someone-knows-bash-far-too-well-and-we-love-it-ivanti-epmm-pre-auth-rces-cve-2026-1281-cve-2026-1340/

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

L’IA découvre des 0-days OpenSSL… pendant que curl arrête son bug bounty

- Une startup (AISLE) affirme avoir trouvé 12 CVE OpenSSL (sur 12)
  - Avec son système IA !
    - Analyse, triage, construction d'exploit (si nécessaire et possible), génération de correctifs et vérification
  - Dont 1 critique avec une potentielle RCE pré-auth
- Certaines vulnérabilités présentes depuis des décennies dans le code
- Première démonstration « réelle » d’AI bug hunting
  - Surtout sur un projet de cette envergure : OpenSSL = code parmi les plus audités au monde
- L’IA dans le monde du bug bounty : avis plutôt négatif
  - Augmente le plafond → vrais 0-days 🥰
    - 13 0-day sur 14 ont été trouvées en 2025 par une IA
  - Effondre la médiane → spam massif de faux rapports 😈 😈
    - Raison pour laquelle curl a arrêté son programme d'ailleurs…

https://www.lesswrong.com/posts/7aJwgbMEiKq5egQbd/ai-found-12-of-12-openssl-zero-days-while-curl-cancelled-its

CVE-2025-15467

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

Log4Shell, Spring4Shell… et maintenant Metro4Shell 👀

- Vulnérabilité se situant dans le composant Metro Development Server utilisé par NPM
  - `@react-native-community/cli`
    - 2 millions de téléchargements par semaine
- Permet une RCE unauthenticated sur le système
  - Via une simple requête POST
- Scénario observé par VulnCheck
  - 1) Exploitation puis injection d'un script PS encodé en Base64
  - 2) Modification de la configuration de Microsoft Defender Antivirus
    - But : exclure l'analyse de *C:\Users\<Username>\AppData\Local\Temp*
  - 3) Liaison avec un C2 pour télécharger un binaire écrit en Rust
    - Comportant des mécanismes « anti-analyses »
- Quelques IoC :
  - 5.109.182[.]231, 223.6.249[.]141 et 134.209.69[.]155
- La vulnérabilité affecte les versions comprises entres 4.8.0 à 20.0.0-alpha.2
  - Passez à la version 20.0.0 de React !

https://www.it-connect.fr/react-native-la-faille-critique-metro4shell-est-exploitee-par-les-cybercriminels/

CVE-2025-11953

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

0-day dans Microsoft 365 / Microsoft Office


CVE-2026-21509

- Permet de contourner les mesures d'atténuation OLE
  - Qui servent à protéger contrôles COM/OLE vulnérables
- Précisions sur la vulnérabilité :
  - L'exploitation est possible uniquement en local sur la machine Windows
  - Le panneau de prévisualisation n'est pas un vecteur d'attaque
  - L'utilisateur doit ouvrir un fichier malveillant via une application de la suite Office
- La vulnérabilité a été ajouté au catalogue KEV de la CISA
- Versions impactées :
  - Office 2016, Office 2019, Office LTSC 2021 et Office LTSC 2024
  - Microsoft 365 Apps (version liée aux abonnements Microsoft 365)
- Processus de MAJ un peu compliqué pour les versions locales, puisqu'il faut aller modifier le registre Windows → https://www.it-connect.fr/microsoft-office-faille-zero-day-cve-2026-21509/

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

Faille critique dans GNU InetUtils

- Composant utilisé pour les accès Telnet
  - Dû à un absence de nettoyage de la variable d'environnement `USER` envoyée en entrée
- Permet d'obtenir un accès root distant sans authentification requise
  - C'est déjà Noël ?
- Comment se réalise l'exploitation ? → `-f root`
- Versions impactées de GNU InetUtils allant de la 1.9.3 à la 2.7
  - Patchez mais… désactivez quand même Telnet (si vous le pouvez)

https://www.it-connect.fr/faille-cve-2026-24061-inetutils-telnet/

CVE-2026-24061

Failles / Bulletins / Advisories
Systeme

Fortinet : exploitation active d’une faille critique

CVE-2025-24155

- Société de renseignement Defused confirme l’exploitation de la vulnérabilité
- OS injection dans le service phMonitor
  - Peut entraîner une RCE unauthenticated
- Plusieurs branches vulnérables → patch disponible

https://www.bleepingcomputer.com/news/security/hackers-now-exploiting-critical-fortinet-fortisiem-vulnerability-in-attacks/

Failles / Bulletins / Advisories
Systeme

RCE 1-Click sur OpenClaw

- Défaut de validation du paramètre gatewayUrl
  - Se situe dans le composant Control UI d'OpenClaw, lié à un mécanisme de connexion automatique
  - Permet à un attaquant d'initier une connexion vers un serveur qu'il contrôle et de récupérer des informations sensibles
  - ET d'aller jusqu'à une exécution de code à distance en 1-Click, si un utilisateur, connecté à son instance OpenClaw, clique sur un lien piégé
- Patch disponible → v2026.1.29 ou v20.26.2.1

https://www.it-connect.fr/openclaw-cve-2026-25253-un-lien-malveillant-suffit-a-executer-du-code-a-distance-en-1-clic/

CVE-2026-25253

Failles / Bulletins / Advisories
Systeme

Stack overflow sur Node.js

CVE-2025-59466

- Possible de faire crasher le serveur
  - Requêtes JSON malveillantes entrainant un code de sortie 7
  - Affecte les applications de production Node.js utilisant l'API async_hooks, dont React Server Components, Next.js…
- Patch disponible

https://thehackernews.com/2026/01/critical-nodejs-vulnerability-can-cause.html

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

HubEE : piratage + fuite de données

- Plateforme d'échanges des flux documentaires entre les différents services de l'État et les usagers
- Intrusion détectée le 9 janvier 2026
  - Possiblement une présence depuis quelques temps déjà
- Estimation de + 70.000 dossiers exportés
  - Soit ~ 160.000 fichiers
- Principaux services visés : DILA, DGCS, DGS, CNAF
- Actions mise en place depuis :
  - Une réinitialisation des mots de passe pour les utilisateurs
  - MFA désormais obligatoire pour les comptes de type "Administrateur"

https://www.it-connect.fr/piratage-hubee-letat-confirme-la-fuite-de-160-000-documents-avec-des-donnees-sensibles/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Retour sur le piratage de Notepad ++

- Grosse suspicion du groupe chinois Lotus Blossom
- De juillet à octobre 2025, modification régulière des adresses de serveurs C2
- Plusieurs sources d'infection ont été identifiés : Vietnam, Savaldor, Australie…
- Même mode opératoire initial : connexion à un serveur et exécution d'un fichier douteux : update.exe
  - Installeur NSIS (Nullsoft Scriptable Install System) qui contient plusieurs fichiers, dont une bibliothèque malveillante (log.dll)
  - Recommandation forte de vérifier la présence du fichier %localappdata%\Temp\ns.tmp
- Modification dans la chaîne d'infection :

Source : Kaspersky

https://www.it-connect.fr/piratage-de-notepad-lotus-blossom-suspecte-derriere-3-vagues-dattaques-distinctes/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

De bonnes pratiques de sécurité mises à l'épreuve

- Détournement de 3 millions € par un employé municipal pendant 4 ans
- Responsable des procédures de contrôle en cas d'anomalie
  - A permis de maquiller ses traces sans être inquiété
- PC du service financier non verrouillé lors de la pause déjeuner
  - Modifiait des coordonnées bancaires ou validait des virements frauduleux, en les faisant passer pour des opérations parfaitement légitimes
  - Redirigait des versements vers des comptes personnels ou des structures intermédiaires comme des associations
- Peine de 2 ans de prison ferme et 24.000 € d'amende

https://www.clubic.com/actualite-595843-millions-d-euros-detournes-de-l-importance-de-verrouiller-sa-session-quand-on-s-absente-de-son-poste.html

Piratages, Malwares, spam, fraudes et DDoS
Piratage

De bonnes pratiques de sécurité mises à l'épreuve (partie 2)

- Victimes inconnues : histoire racontée sur Clubic
  - #UsineFrançaise
  - Que ce soit vrai ou pas, les éléments de l'histoire sont possibles
- Wi-Fi Direct activé sur l'imprimante (acte bienveillant, à priori)
  - Raison : faciliter le travail des prestataires externes
  - « réseau était censé être un bunker numérique isolé du reste du monde, aucune connexion internet, aucune porte de sortie »
- Résultat : un bridge inattendu
  - Plusieurs Go de plans industriels et de formules chimiques confidentielles
    - Représentant 10 ans de R&D
- Segmentez votre réseau ! Même votre imprimante vous veut du mal 💀

https://www.clubic.com/actualite-598513-catastrophe-il-active-le-wi-fi-direct-de-l-imprimante-de-l-entreprise-qui-se-fait-voler-12-go-de-secrets-industriels.html

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

Match Group visé par Shiny Hunter

- Groupe en charge des applications de rencontre
  - Tinder, Hinge, Meetic, Match.com…
- Récupération d'une base de 1.7Go, soit 10 millions d'enregistrements
  - Contient uniquement les utilisateurs de Hinge, Match et OKCupid
- Intrusion liée à la compromission d'un compte SSO via la plateforme Okta
  - A permis aux attaquants d'accéder à AppsFlyer, une solution d'analyse marketing utilisée par Match Group et des données stockées sur Google Drive et Dropbox

https://www.it-connect.fr/une-fuite-de-donnees-chez-match-group-le-geant-derriere-tinder-okcupid-ou-encore-match-com/

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

Données sensibles du Sénégal en ligne

- Piratage du DAF par le groupe The Green Blood
  - Mise en évidence de preuves
- Rappel :
  - DAF, organisme critique qui gère :
    - Les identités des sénégalais et l'identification nationale
    - La biométrie
    - Les données électorales
- Selon un autre rapport, une compromission dans l'AD est présente depuis longtemps
  - Rapport envoyé par la société d'expert cyber IRIS
- Selon le groupe de hackers, 139To de données auraient été exportés
  - À suivre

https://x.com/_SaxX_/status/2019387646104019410

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

Le chef de la CISA un peu trop généreux avec ChatGPT (public)

- Arrivé en juillet 2025
- Documents sensibles non classifiés mais marqués « For Official Use Only » uploadés 🤣
  - Alertes de sécurité déclenchées par les capteurs internes (DLP)
- ChatGPT était bloqué officiellement pour le DHS/CISA
  - Madhu Gottumukkala avait obtenu une autorisation spéciale « short-term »
- Un cas d'école de Shadow AI... même à la CISA !

https://cybersecuritynews.com/cisa-chief-chatgpt/

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

35 millions de données concernées par une fuite de données chez Flickr

- Notification des utilisateurs le 5 février 2026
- Fuite liée à une vulnérabilité chez un fournisseur tiers de services mail
  - Corrigée entre temps
  - Investigation en cours
- Données comprenant :
  - Noms d'utilisateur, adresses mail, types de compte, adresses IP, localisations approximatives, historiques d'activité…
  - Pas de mots de passe ou de numéros de carte bancaire !
- Croisons les doigts pour les 28 milliards de photos / vidéos sur la plateforme 🤞

https://www.clubic.com/actualite-599557-fuite-de-donnee-chez-flickr-35-millions-de-comptes-concernes.html

Piratages, Malwares, spam, fraudes et DDoS
Publication

Net-NTLMv1 définitivement cassé. Même Mandiant le dit.

- Décrit comme étant obsolète depuis 2012, mais toujours beaucoup (trop) utilisé
  - Scénario courant :
    - Auth coercion → capture Net-NTLMv1 → crack hors-ligne
    - Crack possible en quelques heures avec du matériel grand public (< 600$)
- Mandiant veut choquer en publiant des rainbow tables complètes Net-NTLMv1
  - Dataset public (Google Cloud Research Dataset)
  - But : accélérer la disparition de Net-NTLMv1
- Démonstrations + remédiations détaillées dans l'article
  - En bref, désactivez Net-NTLMv1 et forcez l'usage de Net-NTLMv2 😁

https://cloud.google.com/blog/topics/threat-intelligence/net-ntlmv1-deprecation-rainbow-tables?hl=en (article)

https://console.cloud.google.com/storage/browser/net-ntlmv1-tables (rainbow tables)

Piratages, Malwares, spam, fraudes et DDoS
Technique & outil

Blue Team Couper facilement le réseau à un processus

- **ProcNetBlocker** !
  - = Process Network Blocker (CLI)
- 2 modes possibles :
  - Bloquer un processus par son PID
  - Bloquer un exécutable de façon permanente (chemin vers ce dernier)
- Fonctionne sur Windows 7, 8, 10 et 11 ainsi que sur les versions Server

https://autoclose.net/procnetblocker.html

Piratages, Malwares, spam, fraudes et DDoS
Technique & outil

Quand `npm install` vous fait peur

- 1) Lire le code de toutes ses dépendances
- 2) Utiliser **safe-npm**
  - Vérifie si un package a été publié depuis moins de 90 jours ou pas
    - La plupart des compromissions massives ont été détectées et signalées lors des premiers jours / semaines
      - Cf. https://www.ossir.org/paris/supports/2025/2025-10-14/2025-10-14.pdf
      - Cf. https://www.ossir.org/paris/supports/2025/2025-05-13/2025-05-13.pdf
    - `--min-age-days` tout de même disponible..
  - L'outil n'est tout de même pas magique ou divin ! Mais c'est mieux que rien #DefenseEnProfondeur

https://github.com/kevinslin/safe-npm

Business et Politique

Business
Europe

Alerte des autorités allemandes

- La BfV et la BSI indiquent l'utilisation de l'application Signal à des fins néfastes
  - Usurpation du support Signal, avec transmission d'un code PIN par la victime, permet d'enregistrer le compte sur un appareil contrôlé par les attaquants
  - Espionnage des comptes, lié à un scan d'un QRcode par la victime autorisant un appareil des pirates à se connecter au compte Signal
- Recommandations :
  - Vérifier la liste des appareils connectés
  - Supprimer toute connexion inconnue

https://www.linkedin.com/posts/cyber-it-magazine_cybersaezcuritaez-cyberit-signal-activity-7426512712265789440-1oOI?utm_source=share&utm_medium=member_ios&rcm=ACoAABfYHo0BiCBb5qdB1zQWL8DZKwBfAXdSaDQ

Business
Monde

CrowdStrike rachète SGNL (Identity Security)

- Acquisition annoncée : 740 M$
  - Objectif : renforcer la plateforme Falcon côté Identity Security
    - Et sécuriser l'ère Cloud / SaaS / IA
- Ce qu'apporte SGNL :
  - Autorisation dynamique basé sur le risque en temps réel
  - Accès accordé / révoqué en continu
  - Elimination des privilèges permanents
  - Focus sur les identités non humaines / agents IA

https://cybersecuritynews.com/crowdstrike-acquire-sgnl/

Business
Monde

Le NIST repense son rôle dans l'analyse des vulnérabilités logicielles

- Le NIST n'arrive plus à suivre l'explosion du nombre de CVE
  - 20 ans de fonctionnement, le modèle NVD ne scale plus (CVSS, CWE, CPE, etc.)
  - NVD contient ~ 330k CVE | ~29k en attente d'analyse (09/02/2026 à 23h30)
  - « We've been kind of caught on our heels for the last year and a half »
    # Brian Boyen, membre de la division du NVD
- Ne parlons même pas de la crise de financement du programme CVE en 2025
  - Cf. https://www.ossir.org/paris/supports/2025/2025-05-13/2025-05-13.pdf
- Le NIST veut transférer une partie de l'analyse à d'autres acteurs
  - Comme les CNAs
  - Conservation des certaines CVE (KEV CISA, logiciels fédéraux, produits critiques identifiés)

https://www.cybersecuritydive.com/news/nist-cve-vulnerability-analysis-nvd-review/810300/

Droit / Juridique / Politique
Monde

Microsoft donne vos clés de chiffrement BitLocker ???

- Prouvé dans une affaire à Guam lors d'une enquête sur de la fraude
  - Le FBI a eu accès à des postes ayant leurs disques chiffrés avec BitLocker
  - Une commission rogatoire a été envoyée à Microsoft pour récupérer les clés
  - Microsoft a dit oui !
- Cc.. comment ?
  - Lorsque vous activez BitLocker sur un poste, une copie de la clé de récupération est réalisée
    - Et envoyée sur les serveurs de Redmond
      (uniquement si vous utilisez un compte Microsoft)
  - Justification : « au cas où vous oubliez votre mot de passe »
- Apple avait dit non en 2016 dans l'affaire de San Bernardino
  - Mais ce n'est pas le cas pour tout le monde
  - Microsoft dit recevoir 20 requêtes par an mais qu'ils ne peuvent pas toujours y répondre, lol.
- Si jamais, utilisez un compte local ou forcer la sauvegarde local (only) par GPO !

https://www.forbes.com/sites/thomasbrewster/2026/01/22/microsoft-gave-fbi-keys-to-unlock-bitlocker-encrypted-data/

Droit / Juridique / Politique
France

Perquisition pour Elon Musk

- Plateforme X remise en cause
  - Mise à nue des photos transmises sur Grok sans le consentement des personnes concernés
  - Stockage et diffusion de contenu à caractère pédoporngraphique
- Affaire en cours

https://www.lemonde.fr/pixels/article/2026/02/03/les-locaux-francais-de-x-perquisitionnes-dans-le-cadre-d-une-enquete-pour-cybercriminalite_6665203_4408996.html

Droit / Juridique / Politique
France

ANSSI : Stratégie nationale de cybersécurité mise à jour

- Nouvelle version abordant les sujets pour les années à venir 2026-2030
- 2 principes fondamentaux
  - Améliorer nos défenses, et les étendre à tous les pans de la société
  - Mobiliser le collectif, en capitalisant sur des succès déjà réels

https://www.linkedin.com/posts/vincent-strubel-7b7056200_snc2630-activity-7422652097214541825-fGbd

Droit / Juridique / Politique
France

Amende de 5 millions pour France Travail

- Lié aux incidents de 2024
  - Supply chain attack via les comptes d'un prestataire CAP EMPLOI
  - Exfiltration de 20 années de données : numéros de sécurité sociale,adresses mail et postales, numéros de téléphone. PAS DE DONNEES MEDICALES
- 3 négligences pointés du doigt :
  - Une authentification faible
  - Absence de cloisonnement
  - Une journalisation insuffisante
- 5.000€ de plus par jours de retard pour mise en place des remédiations selon planning de la CNIL

https://www.it-connect.fr/la-cnil-inflige-5-millions-deuros-damende-a-france-travail-suite-a-une-fuite-de-donnees-personnelles/

Droit / Juridique / Politique
France

Fin du procès de Free

- Rappel : octobre 2024, compromission du SI de Free avec export de + 24 millions de données
- Vulnérabilités identifiées :
  - Défaillance de sécurité sur le contrôle du VPN
  - Absence de traçabilité globale des actions réalisés
  - Gestion des mots de passe non à l'état de l'art
- Verdict :
  - 27 millions € pour Free Mobile
  - 15 millions € pour Free
- Longue délibération sur la séparation entre les deux entités
  - Notamment pour les clients convergents (utilisateurs des deux plateformes)

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000053352664 (délibération de la CNIL)

https://www.cnil.fr/fr/sanction-free-2026 (publication de la CNIL)

Conférences

Conférences

À venir

- JSSI, 10 mars à Paris
  - Sujet : << **La Supply Chain, maillon faible de la Cyber** >>
- CoRIIN, 31 mars à Lille
  - En parallèle du FIC
- FIC, 31 mars au 2 avril à Lille

Divers / Trolls velus

Divers / Trolls velus

Fin du RC4 « implicite » dans Kerberos

- Aujourd'hui :
  - Comptes avec SPN sans AES → tickets Kerberos négociés en RC4 (implicite)
- À partir de maintenant ?
  - En janvier 2026 : mode audit (nouveaux Event IDs)
  - En avril 2026 : enforcement (AES par défaut, rollback possible)
  - En juillet 2026 : enforcement sans rollback
- Certains équipements ne supportent pas AES, alors attention !
  - OS < Windows 7 / 2008
  - Keytabs générés sans clés AES

  + problèmes de mots de passe (comptes ne possédant pas de clés AES)
  - Mots de passe historiques car inchangés depuis < 2008
  - Comptes migrés avec uniquement les hash NTLM
- Nouveaux Event IDs dans System :
  - 201 / 206 : appareils qui ne supportent pas AES
  - 202 / 207 : comptes nécessitant une réinitialisation de mot de passe

https://techcommunity.microsoft.com/blog/askds/what-is-going-on-with-rc4-in-kerberos/4489365

Divers / Trolls velus

Le projet Sudo a besoin de nous !

- Un seul mainteneur sur le projet Sudo ! Bravo Todd C. Miller 👏
  - 30 ans de maintenance 👏
  - Usage (si jamais) :
    - Permet à un utilisateur autorisé d'exécuter des commandes avec les privilèges d'un autre compte (root ? 👀)
- En recherche de financements
  - Suite à la fin du parrainage de son ancien employeur en février 2024 (filiale de Quest Software)
  - Focus maintenant uniquement sur la correction de bugs et le nettoyage du code
- Canonical a préféré misé sur… sa propre version
  - Sudo-rs → Sudo, mais en Rust
  - Publié en octobre 2025

https://www.it-connect.fr/linux-projet-sudo-a-besoin-de-soutien/

Divers / Trolls velus

Descendant de Linux Torval ou projet Continuity ?

- Projet ayant pour but de succéder à Linux Torval
  - 56 ans maintenant
- Volonté de changer le modèle du Benevolent Dictator for Life (BDFL) par un comité
  - En place depuis 30 ans
  - Comité dirigé par un organisateur puis suivi de son “conclave”
    - Objectif : désigner un ou plusieurs maintainers
  - Le nom de Greg Kroah-Hartman (le bras droit historique de Torvalds) fait beaucoup parler ??

https://www.clubic.com/actualite-597940-linux-un-plan-officiel-pour-succeder-a-linus-torvalds-emerge.html

Divers / Trolls velus

Come back pour Windows 7 et Vista ?

- Nombreuses personnes non satisfaites de windows 10 et 11
  - Solution alternative : passer sous Linux
  - Ressusciter Windows 7 et vista comme le moddeur Bob Pony
- Mise en ligne des ISO des systèmes d'exploitation
  - Disposant des mises à jour de sécurité
- Rappel : version non officielle, plus supporté par Microsoft, plus de nouvelles mises à jour

https://www.frandroid.com/marques/microsoft/2955967_windows-7-et-vista-font-leur-retour-inattendu-en-2026

FIN

Prochaine réunion ?

- RDV le **mardi 13 avril 2026**

Accéder aux différents supports ?

Replays

Slides

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

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