Revue d'actualité de l'OSSIR

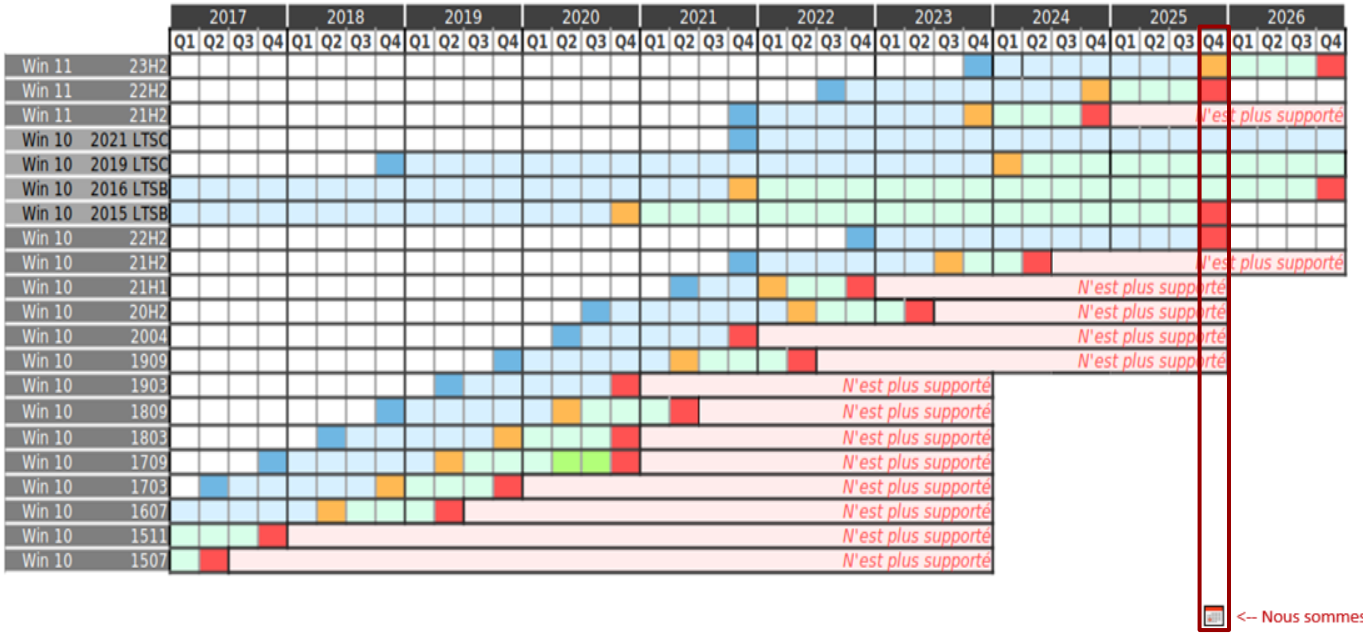
14 octobre 2025

*Jérémy **D**e **C**ock*
*Melchior **C**ourtois*

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

Rappel du support Windows en couleurs

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



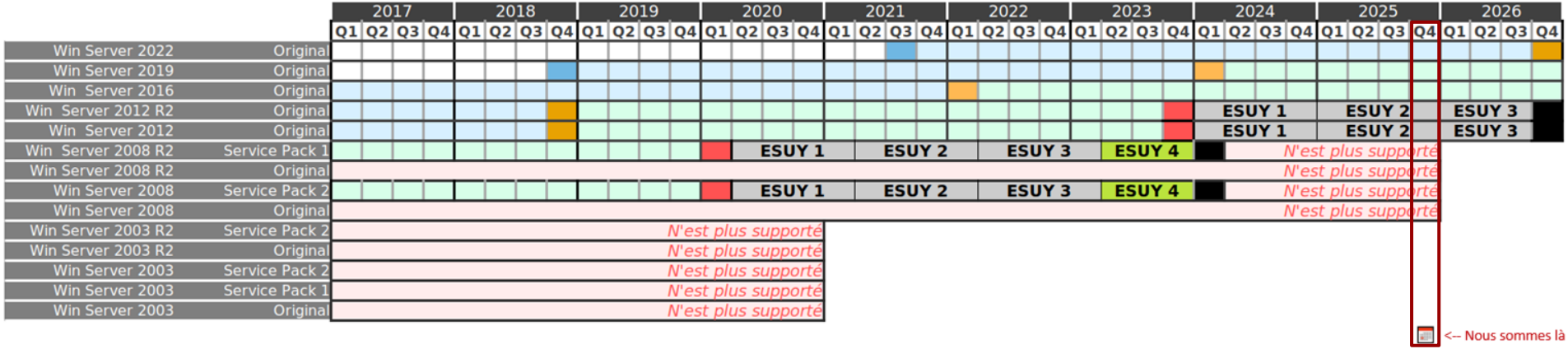
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 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***



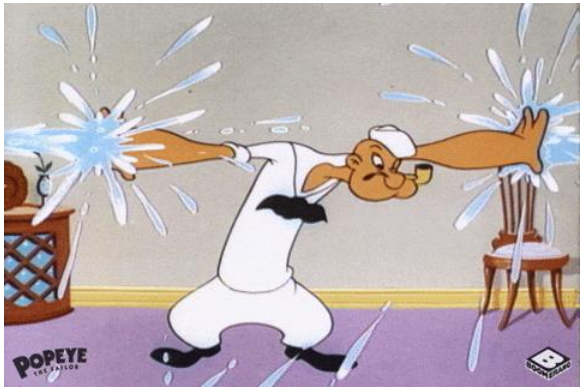
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 septembre, 81 vulnérabilités patchées dont

- 2 vulnérabilités de type 0-day :
  - [**CVE-2025-55234**] Elévation de privilèges, Windows SMB
    - Attaque par relais !
      - Mécanismes de protection existants : SMB Server Signing, EPA
    - Affecte Windows Workstation 10 & 11 ainsi que Windows Server 2008 à 2025
  - [**CVE-2024-21907**] Déni de service, SQL Server
    - Faille située dans la bibliothèque Newtonsoft.Json (versions antérieures à 13.0.1)
      - Enclenchant une exception
    - Réalisable à distance, sans authentification nécessaire
    - Affecte ses versions 2016, 2017 et 2019
- Et 13 failles critiques !

https://www.it-connect.fr/patch-tuesday-septembre-2025-microsoft-recapitulatif/

Failles / Bulletins / Advisories
Système

RCE dans les firewalls Firebox # WatchGuard


CVE-2025-9242

- Type << out-of-bounds write >>
  - Présente dans le processus **`iked`** de Fireware OS
  - Résultat : corruption de la mémoire → exécution de code arbitraire
    - À distance et sans authentification nécessaire !
- Encore faut-il utiliser les VPN IKEv2
- Versions vulnérables :

VERSION VULNÉRABLE	VERSION PATCHÉE
2025.1	2025.1.1
12.x	12.11.4
12.5.x (modèles T15 et T35)	12.5.13
12.3.1 (version certifiée FIPS)	12.3.1_Update3 (B722811)
11.x	Fin de vie

- Modèles associés :
  - T15, T35, T20, T25, T40, T45, T55, T70, T80, T85, T115-W, T125, T125-W, T145, T145-W, T185n M270, M290, M370, M390, M470, M570, M590, M670, M690, M440, M4600, M4800, M5600, M5800, Firebox Cloud, Firebox NV5, FireboxV

https://www.it-connect.fr/watchguard-faille-rce-cve-2025-9242/

Failles / Bulletins / Advisories
Navigateur (principales failles)

0-day dans Google Chrome


CVE-2025-10585

- Type << confusion >>
  - Présente dans le moteur V8
- Patch sorti corrigeant également 3 autres failles
  - [**CVE-2025-10500**] Type "use-after-free" dans Dawn (composant graphique)
  - [**CVE-2025-10501**] Type "use-after-free" dans le composant WebRTC
  - [**CVE-2025-10502**] Type "heap buffer overflow" dans ANGLE
- Vulnérabilité déjà exploitée avant la sortie du patch
- Mettez à jour votre navigateur !
  - Windows / Mac : 140.0.7339.185/.186
  - Linux : 140.0.7339.185

https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html

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

Failles sur équipements CISCO fortement exploitées


CVE-2025-20333


CVE-2025-20362

- Produits concernés :
  - Cisco ASA et FTD (appliances de pare-feu / VPN web-interface)
- Quid des failles ?
  - [**CVE-2025-20333**] RCE unauthenticated
  - [**CVE-2025-20362**] Accès (non authentifié) à des endpoints restreints liés au VPN
- Shadowserver a détecté ~48.800 ASA/FTD exposés et vulnérables
- TTPs observés : déploiement d'un loader Line Viper suivi d'un bootkit RayInitiator
- Priorité 0 : appliquer les correctifs Cisco publiés
  - Si ce n'est pas possible :
    - Déconnecter les appliances obsolètes
    - Limiter l'accès VPN web-interface (ACL/geo-block)
    - Surveiller les tentatives d'accès

https://www.bleepingcomputer.com/news/security/nearly-50-000-cisco-firewalls-vulnerable-to-actively-exploited-flaws/

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

Faille 0-day sur la solution Oracle E-Business Suite


CVE-2025-61882

- Se situe dans le composant `Oracle Concurrent Processing`
  - RCE possible sans authentification requise !
- Exploitée par le groupe Cl0p
  - Le but étant de voler des données sur les serveurs de plusieurs organisations
    - Accompagné de la réception (pour les victimes) d'un mail d'extorsion
  - IoC publiés par Oracle : 200[.]107[.]207[.]26 et 185[.]181[.]60[.]11
- Versions affectées : 12.2.3 à 12.2.14

https://www.it-connect.fr/oracle-cve-2025-61882-zero-day-ransomware-clop/

Failles / Bulletins / Advisories
Applications (principales failles)

RCE sur GoAnywhere

CVE-2025-10035

- Patch disponible le 18 septembre
  - Trace d’attaque depuis le 11 septembre
  - V7.8.4 ou v7.6.3 pour la version Sustain Release
- Vulnérabilité sur le service de gestion des licences
  - Faiblesse liée à la désérialisation : en forgeant une signature de réponse de licence, un attaquant peut contourner la vérification de l'intégrité et injecter un objet malveillant
- Rappel : NE PAS EXPOSER SES INTERFACES D’ADMIN SUR INTERNET

http://it-connect.fr/faille-critique-goanywhere-cve-2025-10035-attaques-ransomware/

Failles / Bulletins / Advisories
Applications (principales failles)

Coup dur pour Redis

CVE-2025-49844

- Use-after-free dans l'interpreteur Lua de Redis
  - Affecte toutes les versions de Redis supportant l'interpréteur et activé par défaut
- Manipulation du garbage collector pour échapper à la sandbox Lua puis déploiement d'un reverse-shell pour un accès distant persistant
  - Peut mener à une RCE sur le serveur
- Besoin d'être authentifié pour exécuter la vulnérabilité normalement
  - Cependant authentification optionnelle sur ⅕ (60.000) des instances en ligne
- Patch disponible → v8.2.2

https://www.it-connect.fr/redishell-faille-de-securite-critique-redis-cve-2025-49844/

Failles / Bulletins / Advisories
Equipements (principales failles)

Adieu FreeWifi_Secure

- Fonctionnalité des box Free afin de délivrer un wifi pour tous les abonnés
  - Authentification par carte SIM (protocole EAP-SIM)
  - Problème : envoi de l'IMSI en clair (numéro d'identifiant unique) afin établissement d'un canal sécurisé
- Free a demandé à retarder la divulgation, le temps de déployer un correctif
  - Patch du 1er octobre : désactivation par défaut du service FreeWifi_Secure sur tous les modèles de Freebox concernés
- Services non présents sur les box Free récentes (Pop, Delta, Ultra)

https://www.it-connect.fr/adieu-freewifi_secure-une-faille-de-securite-a-accelere-sa-fin/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Accès frauduleux à des sauvegardes Cloud de firewall SonicWall

- Que s'est-il passé ?
  - Attaque par brute-force réalisé pour accéder à des comptes MySonicWall
  - Résultat : main mise sur des fichiers de config de pare-feu de SonicWall appartenant à des clients
- Fichiers de configuration sauvegardés via la fonction Cloud Backup
  - On peut y retrouver : identifiants (avec les mots de passe chiffrés), jetons, clés de chiffrement, etc.
- Compromission possible des firewalls (victimes)
  - Sauf si l'interface de gestion n'est pas libre d'accès depuis le WAN 😊
  - Réinitialisez quand même vos identifiants !

https://www.bleepingcomputer.com/news/security/sonicwall-warns-customers-to-reset-credentials-after-MySonicWall-breach/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

SORVEPOTEL, le malware WhatsApp

- Incite l'utilisateur à télécharger le ZIP sur PC et l'ouvrir
  - Contient un fichier de raccourci (.LNK), avec un script qui télécharge le code malveillant principal du malware surnommé SORVEPOTEL
  - Persistance sur l'équipement et propagation sur les contacts du WhatsApp
- Objectif : récupérer des informations de la victime (keylogger, photos…)
  - Présent dans 95% des cas au Brésil

https://www.it-connect.fr/whatsapp-le-malware-sorvepotel-se-propage-automatiquement-a-tous-les-contacts/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Accès frauduleux sur la plateforme Google dédiée aux autorités américaines 

- Compte frauduleux créé sur la plateforme en question (LERS)
  - Accès au système de demande judiciaire pour les forces de l'ordre
    - Utilisée par les agence de police et de renseignements
  - Origine : Scattered Lapsus$ Hunters
- Le FBI ne s'est pas exprimé sur le sujet
  - On parle quand même d'accès à des informations sensibles comme des casiers judiciaires…
- Compte supprimé + affirmation qu'aucune donnée n'a été consultée
  - Des copies d'écran partagées circulent tout de même sur Telegram

https://www.bleepingcomputer.com/news/security/google-confirms-fraudulent-account-created-in-law-enforcement-portal/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Piratage intense en cours dans les lycées des Hauts-de-France

- Près de 80 % des lycées publics de la région sont actuellement touchés
  - Données techniques visées
  - Accompagnés par Orange Cyber Défense
- Liée au groupe Qilin
  - +1.000 Go de données
    - dont des pièces d'identité en tout genre, des relevés de notes, CV, et autres données personnelles
    - Echantillon offert sur le dark web
  - Connu pour effectuer de la double extorsion

https://www.hautsdefrance.fr/incident-de-cybersecurite-dans-plusieurs-lycees-de-la-region-hauts-de-france/

Piratages, Malwares, spam, fraudes et DDoS
Supply-chain

Compromission de 20 packages npm ultra-populaires

- Compte mainteneur (alias Qix, Josh Junon) victime d'un phishing ciblé
  - L'incitant à réinitialiser sa 2FA
  - Merci le faux support npm
- Publication (malveillante) de 20 packages npm
  - Cumulant 2 milliards de téléchargement hebdomadaires…
- But du code malveillant inséré :
  - Intercepter ou détourner les transactions de crypto monnaies dans le navigateur
    - Modification d'adresses de destination et/ou manipulation silencieuse
- HEUREUSEMENT : anomalie détectée dans les 5 minutes (merci Aikido Security)
  - Alerte publiée dans l'heure

https://thehackernews.com/2025/09/20-popular-npm-packages-with-2-billion.html

Piratages, Malwares, spam, fraudes et DDoS
Malware

ClayRat, le malware Android

- Imitation de sites légitimes incitant l'utilisateur à télécharger l'APK
  - Installation de ClayRat, en tant que dropper
  - Installe ensuite furtivement un malware sans alerter l'utilisateur
    - ex : avec un faux écran de mise à jour
- Permet de faire de la récupération d'informations en masse :
  - Inventaire des applications installés, journaux d'appel et SMS, prendre une photo, envoyer des informations depuis la machine…
- Cible en priorité les utilisateurs en Russie pour le moment

https://www.it-connect.fr/android-le-malware-clayrat-cible-les-utilisateurs-de-whatsapp-et-youtube/

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Attaque par ransomware réalisée dans plusieurs aéroports

- Grands aéroports européens affectés dont Londres-Heathrow, Bruxelles, Berlin-Brandebourg
- Impact direct sur le système MUSE de Collins Aerospace
  - Système hors-service : plus de check-in ou d'enregistrement possible
  - Plan B : retour au papier !
- Arrêt total du trafic aérien évité, mais des centaines de vol retardés ou annulés
- Aucune information aujourd'hui sur la source de l'attaque

https://www.it-connect.fr/ransomware-plusieurs-aeroports-europeens-perturbes-par-une-cyberattaque/

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Le retour de LockBit en 5.0

- Peut chiffrer les données de machines sous Windows, Linux, ou VMware ESXi
- Evolution de LockBit 4.0
  - Similitudes notamment avec les algorithmes de hachage et les méthodes de résolution d'API
  - Diffusé en tant que RaaS (Ransomware-as-a-Service)
- Utilise une technique d’obfuscation et un compactage plus avancé
  - Détection difficile avec
    - Des extensions de fichiers aléatoires de 16 caractères
    - La suppression des journaux d'événements de la machine, après l'opération de chiffrement
    - L'exclusion des fichiers en langue russe

https://www.it-connect.fr/ransomware-lockbit-5-0-une-nouvelle-menace-pour-windows-linux-et-vmware-esxi/

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

Huawei Tech. sous une fuite majeure

- Incident début octobre avec mise en vente des informations :
  - Fichiers de code source (ex.: .c, .cpp, .h, .pas)
  - Outils et scripts de développement interne
  - Créer des fichiers et des configurations (ex.: makefile, confs .ini)
  - Documentation technique et manuels

https://dailydarkweb.net/huawei-technologies-source-code-exposed-in-data-breach/

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

Renault touché par un prestataire

- Cyberattaque chez un prestataire le 3 octobre
  - Maîtrisée selon Renault
  - Aucun système compromis chez Renault
- Contenu des informations fuitées
  - Noms, adresses, dates de naissance, sexe, numéros de téléphone, numéros d'identification des véhicules et détails d'immatriculation des véhicules
  - Aucune information contenant des informations financières ou des mots de passe

https://www.ouest-france.fr/societe/cyberattaque/noms-adresses-numeros-de-telephone-les-donnees-de-clients-renault-derobees-au-royaume-uni-937eb7c0-a04c-11f0-8fee-8372019c9cea

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

Fuite gravissime pour les utilisateurs de Discord

- Cyberattaque le 20 septembre 2025 sur Zendesk, l'outil de support client de Discord
  - Maîtrisé selon Discord
  - Aucune compromission directe de ses serveurs
  - Accès frauduleux durant 58 heures via le compte d'un agent
    - Désactivation de la MFA et exfiltration des données
- Contenu des informations fuitées
  - Noms d'utilisateur, adresses mail, adresses IP, messages envoyés au support, pièces jointes, documents d'identité * et 4 derniers chiffres des cartes bancaires
  - Les mots de passe ne sont pas concernés
- Discord évoque 70.000 utilisateurs touchés
  - Les pirates revendiquent 5,5 millions et 1,6 To de données volées

https://www.theregister.com/2025/10/06/discord_support_data_breach/

* Les pirates affirment qu'ils ont récupérés 521.000 tickets de vérification de l'âge 😱

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

Rumeur de fuite massive de données de l'ANTS

- Base de données prétendument issue de l'ANTS mise en vente sur le dark web
  - En réalité, elle circule depuis mars 2025 (au moins)
  - Contient des données personnelles (identités, contacts…) mais
    - Aucun lien confirmé avec les systèmes ou bases de l'ANTS !
- Message de Vincent Strubel (ANSSI) :
  - `<< Les cybercriminels sont assez forts comme ça en marketing, inutile de leur faire de la pub gratuite. >>`
  - `<< Pensée pour les équipes de l'ANTS qui ont passé le week-end à tout revérifier, sans spectacle. >>`
- Attention à ce que vous trouvez sur les réseaux :
  - Risque d'impact réputationnel fort malgré l'absence de compromission prouvée (= diffamation)

https://www.linkedin.com/posts/vincent-strubel-7b7056200_cp-ants-ugcPost-7375854480896081920-jV6V

Piratages, Malwares, spam, fraudes et DDoS
Publication

Maturité cyber des TPE-PME 2025

- Merci cybermalveillance.gouv.fr
- Quelques chiffres marquants :
  - 16 % des TPE/PME déclarent avoir subi un ou plusieurs incidents cyber au cours des 12 derniers mois
  - 44 % estiment être fortement exposés aux risques cyber (vs 38 % en 2024)
  - 58 % pensent bénéficier d'un bon ou très bon niveau de protection (vs 39 % en 2024)
  - Moyenne de dispositifs de sécurité installés : 4,06 (vs 3,62 en 2024)
  - Dispositifs les plus fréquents : antivirus 84 %, sauvegardes 78 %, pare-feu 69 %
  - 24 % des TPE/PME affirment disposer de procédures de réaction aux cyberattaques (+5 pts en 1 an)
  - 80 % reconnaissent qu'elles ne sont pas prêtes aux attaques ou l'ignorent encore
  - Principaux freins à une meilleure sécurité :
    - 63 % par manque de connaissances / expertise
    - 61 % pour des contraintes budgétaires
    - 59 % par manque de temps
  - 15 % prévoient d'augmenter leur budget cybersécurité (pour ¾, budget < 2 000 €)
  - 6 entreprises sur 10 ont déjà engagé des actions de sensibilisation
- Une progression perceptible, mais toujours un cap à franchir !
- Beaucoup de TPE/PME sont encore dans une posture << réactive >> plutôt que << préventive >>

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/etude-maturite-cyber-tpe-pme-2025

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

Red Team Outil capable de suspendre les solutions de sécurité sur Windows

- Outil en question : EDR-Freeze (https://github.com/TwoSevenOneT/EDR-Freeze)
- Permet de neutraliser les solutions de type EDR et les antivirus…
  - … dans le contexte d'un utilisateur standard !
- Utilisation de deux composants :
  - Windows Error Reporting (WER) : système de rapport d'erreurs de Windows
    - Conçu pour collecter des informations sur les incidents et les envoyer à Microsoft
  - API MiniDumpWriteDump : fonction de la bibliothèque DbgHelp
    - Sert à générer une image instantanée de la mémoire et de l'état d'un processus

      ⚠️ Pour garantir la cohérence des données : tous les threads du processus sont temporairement suspendus
- Scénario réalisé (race-condition) :
  1. Utilisation du composant `WerFaultSecure` (privilèges élevés)
  2. Appel à l'API `MiniDumpWriteDump` sur un processus sécurité
  3. Suspension (le timing doit être parfait) de `WerFaultSecure`

  → Processus sécurité dans un état de << coma >>
- L'outil est capable de neutraliser Windows Defender sur Windows 11 24H2

https://www.it-connect.fr/edr-freeze-suspendre-solutions-de-securite-grace-a-windows-wer/

Business et Politique

Business
Monde

1 an de sursis pour Windows 10, en Europe

- Le support technique de Windows s'arrête le 14 octobre
  - 10 ans de support effectué pour Windows 10 ET Windows 11 est là
  - OK. mais…
- 2 gros problèmes :
  - Impossible d'installer Windows 11 sur des machines << anciennes >> (= n'ayant pas de puce TPM 2.0)
    - Jusqu'à 850 millions de machines concernées (selon l'association HOP)
    - Listes cadeau :
      - https://learn.microsoft.com/fr-fr/windows-hardware/design/minimum/supported/windows-11-supported-intel-processors
      - https://learn.microsoft.com/fr-fr/windows-hardware/design/minimum/supported/windows-11-supported-amd-processors
  - 4 ans se sont écoulées depuis l'arrivé de Windows
    - ≠ 8 ans entre l'arrivé de Windows 10 et la fin de support de Windows 8/8.1
- Conditions pour l'ESU :
  - Avant :
    - Soit payer 30 $, soit payer 1.000 points Microsoft Reward, soit utiliser l'outil de sauvegarde en ligne
  - Maintenant :
    - Pour les européens : se connecter sur sa machine avec son compte Microsoft
      - Fin de support prévu en octobre 2026

https://next.ink/201508/windows-10-obtient-un-an-de-sursis-en-europe-en-quelque-sorte/

Droit / Juridique / Politique
Monde

Microsoft retire ses services Cloud à l'unité 8200 israélienne

- Enquête conjointe de +972 Magazine / Local Call / The Guardian
- L'unité 8200 (renseignement militaire israélien) stockait ses données sur Azure
  - Données en question : des millions d'appels interceptés de Palestiniens
  - Données utilisées pour des frappes ciblées et des opérations d'arrestation
- Réponse de Microsoft après la réalisation d'une enquête interne :
  - Suspension partielle de l'accès Azure pour l'unité
  - Première fois qu'un GAFAM coupe l'accès à une entité militaire israélienne !
- Réponse de l'unité 8200 ; migration de ses données vers AWS
  - Est-ce que Amazon va suivre le mouvement ?

https://www.972mag.com/microsoft-cloud-israel-8200-expose/

Droit / Juridique / Politique
France

Retour sur le piratage d'Adecco

- Victime de piratage en 2022 avec fuite de données
  - +100.000 victimes
  - Nombreuses accusations : escroquerie en bande organisée, blanchiment, fabrication de faux papiers d'identité, ou encore atteinte à des systèmes de données
- 15 prévenus comparaissent
  - Timothée Lhomond (20a): chef du réseau et CEO d'une boîte de gestion de fuite de données 😳
- Verdict du procès : 6 ans de prison ferme et 30.000 € d'amende
  - 6 mois à 3 ans de prison pour ses complices
- Partie civile en attente de dédommagement pour dommages et intérêts

https://www.numerama.com/cyberguerre/2085819-le-verdict-est-tombe-pour-le-gang-de-jeunes-hackers-francais-derriere-le-piratage-dadecco-retour-sur-une-affaire-hors-normes.html

Business
Monde

Initiative de l'Arcom

- Ciblage des services IPTV et streaming
  - Demande récente aux fournisseurs VPN de bloquer ~300 sites de diffusion de sport
  - + 5.000 serveurs bloqués depuis le début de l'année
    - Permet de neutraliser efficacement un ensemble de revendeurs et de petites plateformes locales
- Efficacité des VPN diminuée
  - Moins de confidentialité et neutralité
  - Les fournisseurs comprennent l'enjeu de freiner le piratage, mais refusent de devenir des censeurs

https://www.lesnumeriques.com/vpn/la-fin-du-piratage-en-france-l-arcom-s-attaque-aux-vpn-n243272.html

Conférences

Conférences

Passée(s)

- FranSec, 16 au 17 septembre 2025 à Paris
- Kernel Recipes, 22 au 24 septembre 2025 à Paris
- WineRump, 26 septembre 2025 à Bordeaux
- Les Assises, 08 au 11 octobre 2025 à Monaco
- Hexacon, 10 au 11 octobre 2025 à Paris
- SecSea2k5, 10 au 11 octobre 2025 à La Ciotat

À venir

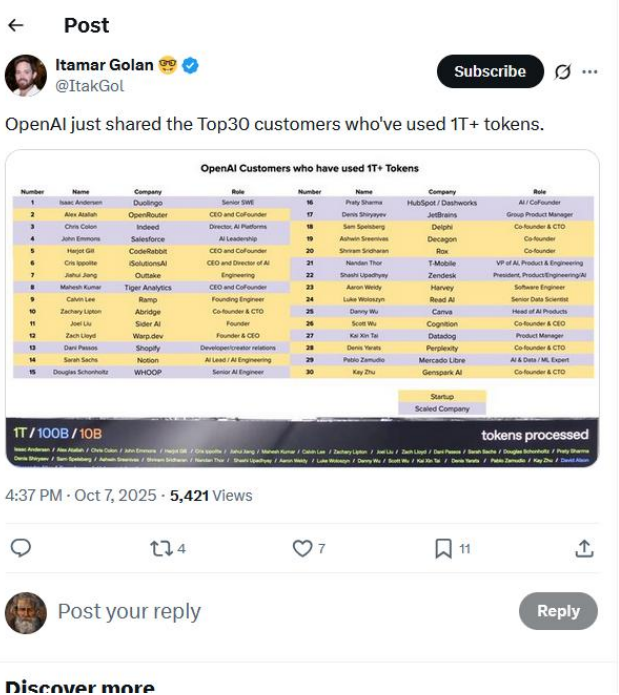
- FIC, 14 au 15 octobre 2025 au Canada
- Identity Days, 21 octobre 2025 à Paris
- Unlock your brain, 7 au 8 novembre 2025 à Brest
- European Cyber Week (ECW), 17 au 20 novembre à Rennes
- GreHack, 28 au 29 novembre 2025 à Grenoble

Divers / Trolls velus

Divers / Trolls velus

TOP 30 clients de OpenAI ayant utilisés plus de 1 trillion de tokens (10^{12})

- Liste partagée (ou fuite non confirmée) sur la communauté OpenAI
- Quelques noms marquants :
  - Duolingo, Salesforce, Shopify, Zendesk, Datadog, Notion, etc.
- Usages probables :
  - Chatbots, analyse, assistants, génération, etc.
- Interprétation ?
  - Industrialisation déjà en cours de l'usage des LLM
  - Consommation à très grande échelle (core business)



https://community.openai.com/t/openai-just-shared-the-top30-customers-whove-used-1t-tokens/1361452/2

Divers / Trolls velus

Windows – Expiration des certificats Secure Boot & mises à jour CA

- Que fait le Secure Boot (via UEFI) ?
  - Garantit que seuls les composants signés et de confiance s'exécutent au démarrage
    - Bootloaders, firmware, modules UEFI
- Comment ?
  - Le firmware utilise des certificats KEK, DB, DBX, gérés par Microsoft & partenaires
- Ce qu'il faut prévoir :
  - *Microsoft Corporation KEK CA 2011* → expiration en juin 2026
  - *Microsoft Windows Production PCA 2011* → expiration en octobre 2026
  - *Microsoft UEFI CA 2011* → expiration en juin 2026
  - *Microsoft Option ROM CA 2011* → expiration en juin 2026
- Ce qu'il faut retenir :
  - `<< En 2026, les certificats Secure Boot de Microsoft arrivent à expiration — sans mise à jour vers les versions 2023, les machines Windows risquent de perdre les mises à jour de sécurité du mécanisme de boot. >>`

https://support.microsoft.com/en-gb/topic/windows-secure-boot-certificate-expiration-and-ca-updates-7ff40d33-95dc-4c3c-8725-a9b95457578e

Divers / Trolls velus

The Great Chinese Firewall is online

- ~ 600 Go de données sur la technologie de la censure en Chine
  - Tout le code source, les documents internes, les logs de travail et même les communications privées
- 2 sources distinctes :
  - Geedge Networks, une boîte dirigée par Fang Binxing (surnommé le << père du Great Firewall >>)
  - Le laboratoire MESA de l'Académie chinoise des sciences
- Information sur la vente de l'équipement à d'autres pays comme la Birmanie, le Pakistan, l'Ethiopie ou le Kazakhstan

https://korben.info/great-firewall-chinois-vient-prendre-500.html

Divers / Trolls velus

Bonne nouvelle pour YesWeHack

- Officiellement devenue une CNA le 23 septembre 2025
  - Lui permet d'attribuer directement des identifiants CVE à des vulnérabilités découvertes
  - Comme Dassault, Schneider, Thales ou WPScan
- Reconnaissance + accélération des flux entre les bounty hunters et les organisations clientes
  - + Renforcement de sa position dans l'écosystème cyber français et international (cocorico)

https://www.cve.org/PartnerInformation/ListofPartners (liste des CNA dans le Monde)

https://www.clubic.com/actualite-580342-le-francais-yeswehack-denicheur-de-vulnerabilites-informatiques-entre-dans-la-cour-des-grands.html

Divers / Trolls velus

Encore un record battu pour Cloudflare

- Atténuation de la plus grosse attaque DDoS à ce jour
  - Dernière en date il y a 3 semaines par eux déjà
  - Attaque d'une durée de 40 secondes
    - avec 22.2 Tbs
    - et 10.6 milliards de paquets par seconde
- Attaque qui serait liée au bot AISURU
  - Cible en priorité les routeurs et les objets connectés (caméras, enregistreurs, puces…)

https://www.it-connect.fr/cloudflare-attenue-une-nouvelle-attaque-ddos-record-222-tbps/

FIN

Prochaine réunion ?

- RDV le **mercredi 12 novembre 2025**

Accéder aux différents supports ?

Replays

Slides

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

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