Revue d'actualité de l'OSSIR

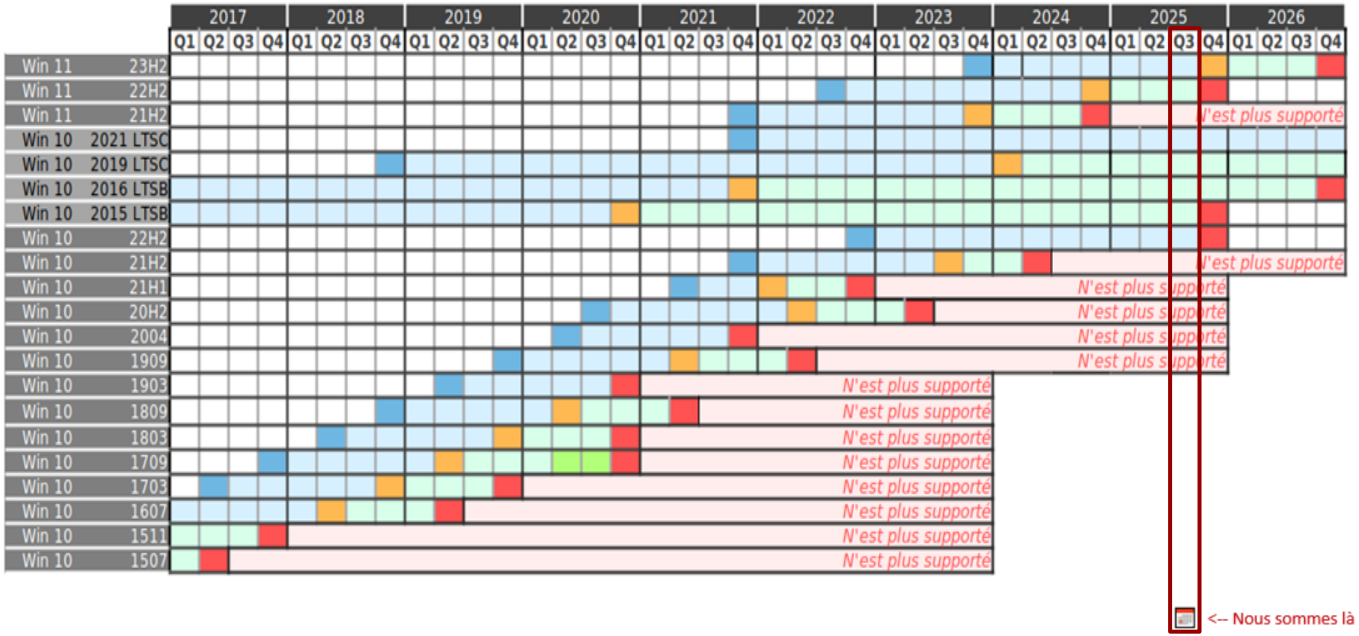
09 septembre 2025

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***



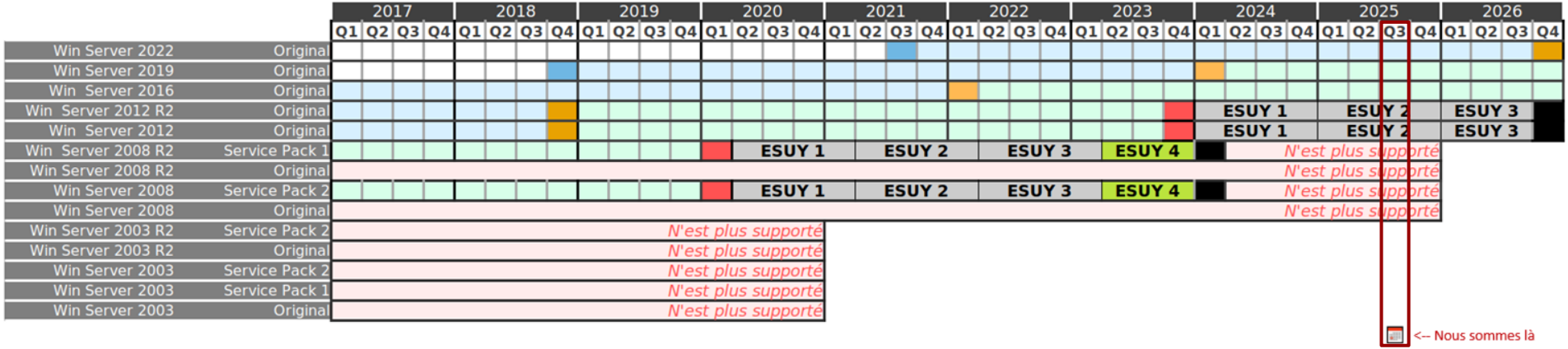
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



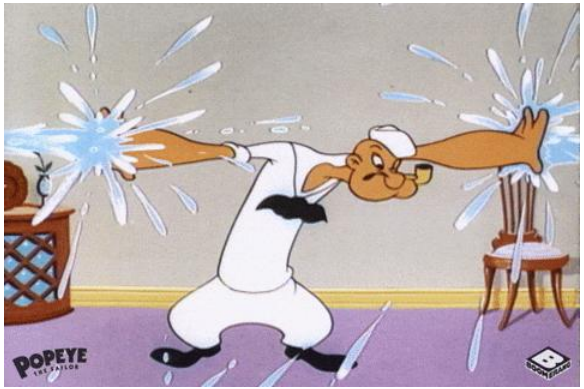
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 juillet, 137 vulnérabilités patchées dont

- 1 vulnérabilité de type 0-day :
  - [**CVE-2025-49719**] Leak d'informations (sur le réseau), Microsoft SQL Server
    - N'est pas exploitée selon Microsoft
    - Affecte les versions 2016, 2017, 2019 et 2022
- Les plus critiques ou les plus intéressantes :
  - **16** vulnérabilités dans les services de routage et d'accès distant de Windows Server (RRAS)
  - [**CVE-2025-49697,49695,49696,49702**] RCE, Microsoft Office
    - Ne nécessitent pas d'interaction utilisateur
    - Ne sont pas exploitées selon Microsoft

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

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin d'août, 107 vulnérabilités patchées dont

- 1 vulnérabilité de type 0-day :
  - [**CVE-2025-53779**] Élévation de privilèges (sur le réseau), Windows Kerberos
    - Divulguée publiquement par des chercheurs
    - Nécessite une authentification préalable (utilisateur)
    - Affecte Windows Server 2025
- Les plus critiques ou les plus intéressantes :
  - **5** vulnérabilités dans Hyper-V et **5** dans Exchange
  - [**CVE-2025-53778**] Élévation de privilèges, Windows NTLM
    - Ne sont pas exploitées selon Microsoft

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

Failles / Bulletins / Advisories
Navigateur (principales failles)

Faille critique sur les navigateurs

CVE-2025-6558

- Identifiée par le Google Threat Analysis Group
- Vulnérabilité activement exploitée
  - Défaut de validation des entrées dans les composants ANGLE et GPU
  - Permet d'échapper la sandbox du navigateur (à distance) → exécution de code
- Affecte :
  - Chrome < 138.0.7204.157/158
  - Edge (Chromium) < 138.0.3351.95
  - Safari (iOS 18.6, macOS 15.6, etc.)
- Patchs disponibles

https://socprime.com/blog/cve-2025-6558-google-chrome-vulnerability/

Failles / Bulletins / Advisories
Navigateur (principales failles)

Clickjacking DOM, l'ennemi des gestionnaires de mots de passe

- Présentée lors d'une conférence de la DEF CON 33
- Scénario :
  - Superposition d'un formulaire de connexion invisible sur le bouton d'une bannière
  - Click ! (sur le bouton invisible de remplissage automatique du gestionnaire de mots de passe)
  - Identifiants insérés dans le formulaire caché et immédiatement exfiltrés vers un serveur ☠️
- 11 extensions populaires testées ont été identifiées comme vulnérables
  - Autofill automatique = aucun clic !
  - Autofill manuel = choix de l'identifiant depuis une liste
- Sites de démo : https://marektoth.com/blog/dom-based-extension-clickjacking/
  - + versions patchées
- Bonnes pratiques :
  - Verrouillage auto du coffre en cas d'inactivité
  - Désactiver la fonction de remplissage automatique
  - Utiliser un paramétrage strict pour la détection du domaine

https://korben.info/vos-gestionnaires-mots-passe-pieges-simple.html

Password Manager	Credit Card	Personal Data	Login	TOTP	Passkeys
1Password	✓	1 click	1 click	0 click	1 click
Bitwarden	1 click	1 click	1 click	0 click	✓
Dashlane	✓	✓	✓ *	✓	1 click
Enpass	1 click	1 click	1 click	0 click	✓
iCloud Passwords	Not supported	Not supported	1 click	1 click	✓
Keeper	5 clicks	5 clicks	1 click	0 click	1 click
LastPass	2 clicks	2 clicks	2 clicks *	0 click *	1 click
LogMeOnce	1 click	1 click	1 click *	0 click *	1 click
NordPass	1 click	1 click	1 click	✓	1 click
ProtonPass	Not supported	1 click	1 click	1 click	1 click
RoboForm	1 click	1 click	1 click	1 click	1 click

Password Manager	Credit Card	Personal Data	Login	TOTP	Passkeys
✗ 1Password	✓	1 click	INFORMATIVE	0 click	1 click
✗ Bitwarden	1 click	1 click	IN PROGRESS	0 click	✓
✓ Dashlane*	FIXED				
✗ Enpass	1 click	1 click	IN PROGRESS	0 click	✓
✗ iCloud Passwords	Not supported	Not supported	IN PROGRESS	1 click	✓
✓ Keeper	FIXED				
✗ LastPass	FIXED		2 clicks *	INFORMATIVE	1 click
✗ LogMeOnce	1 click	1 click	NOT FIXED - NO EMAIL REPLY	0 click *	1 click
✓ NordPass	FIXED				
✓ ProtonPass	FIXED				
✓ RoboForm	FIXED				

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

0-day activement exploitée sur les équipements Apple

CVE-2025-43300

- Type << out-of-bounds write >> sur le composant Image IO
  - Fichier image piégé → corruption de données | panne | exécution de code
- `<< [...] attaque extrêmement sophistiquée contre des individus spécifiquement ciblés >> #Apple`
- Affecte :
  - iOS < 18.6.2
  - iPadOS < 17.7.10
  - iPadOS < 18.6.2
  - macOS Sequoia < 15.6.1
  - macOS Sonoma < 14.7.8
  - macOS Ventura < 13.7.8

https://gbhackers.com/cisa-warns-of-actively-exploited-0-day-vulnerability-in-apple/

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

RCE dans le RADIUS de FMC #CISCO

CVE-2025-20265

- Vulnérabilité dans le Secure Firewall Management Center de CISCO
  - Plus particulièrement dans son sous-système RADIUS
    - Mauvaise validation des identifiants reçus
    - L'authentification RADIUS doit donc être activée !
  - Permet une RCE unauthenticated
- Versions 7.0.7 et 7.7.0 de FMC affectées - patchez !
  - En attendant, possible de désactiver RADIUS ou de changer de méthode d'authentification
    - Alternatives : comptes locaux, LDAP, ou SSO SAML
- Aucune exploitation connue dans la nature à la date de divulgation

https://thehackernews.com/2025/08/cisco-warns-of-cvss-100-fmc-radius-flaw.html?ref=veillecyber.fr

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

Crash de 7-Zip

CVE-2025-53816

- Vulnérabilité dans la fonction de réparation d'une archive RAR5 corrompue
  - Fonction << NCompress::NRar5::CDecoderw >>
    - << My_ZeroMemory(_window + _winPos, (size_t)rem) >>
    - Variable rem manipulable, pas de limite de taille
- Possible de faire crasher l'application 7-Zip
  - Risque pour les systèmes d'analyse qui s'appuieraient sur les composants de 7-Zip pour opérer
- Patch disponible → v25.00

https://www.it-connect.fr/7-zip-cve-2025-53816-faille-archive-rar5/

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

HPE Aruba : point d'accès vulnérable

CVE-2025-37102
CVE-2025-37103

- 2 failles critiques permettant de prendre le contrôle de l'équipement
  - Injection de commande via un accès authentifié
  - Identifiés codé en dur dans l'interface de gestion
- Patch disponible → v3.2.0.1

https://www.it-connect.fr/hpe-aruba-patchez-vos-points-dacces-wi-fi-pour-eliminer-ces-identifiants-codes-en-dur/

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

Docker Desktop, faille SSRF

CVE-2025-9074

- Permet à un conteneur malveillant d'accéder au système hôte
  - Lié à l'API Docker Engine
    - Accessible depuis le conteneur (192.168.65.7:2375)
    - Sans authentification
    - Pourrait créer et démarrer un nouveau conteneur qui monte le lecteur C: de l'hôte Windows à partir de requêtes POST
- Affecte les versions v4.25 à v4.44.2
  - Patch disponible → v4.44.3
- Faille moins impactante sur macOS

https://www.it-connect.fr/cve-2025-9074-cette-faille-critique-dans-docker-desktop-permet-de-pirater-windows/

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

CVE-2025-...

Montée de version sur GLPI : 10.0.19

- Update centrée sur la correction des failles de sécurité
  - Jusqu’à 9 failles corrigées
  - Aucune identifiée comme critique
- Aucun détail technique n’a été communiqué

https://www.it-connect.fr/passez-sur-glpi-10-0-19-pour-vous-proteger-de-ces-9-failles-de-securite/

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

Faille potentiellement critique chez Plex Media Server

- Identifiée dans le contexte d'un programme de Bug Bounty
  - Pas de détails techniques
  - Communication faite aux clients par mail (inhabituelle pour Plex)
- Patch disponible depuis le 11 août → v1.42.1.10060

https://www.it-connect.fr/patchez-plex-media-server-protegez-votre-serveur-de-cette-faille-de-securite/

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

4 failles sur VMware ESXi et Workstation

CVE-2025-41236
CVE-2025-41237
CVE-2025-41238
CVE-2025-41239

- GROSSES failles :
  - Affectent respectivement les adaptateurs VMXNET3, le module VMCI, le contrôleur PVSCSI et le processus vSocket
  - Permet à l'aide des droits administrateur d'exécuter du code malveillant sur l'hôte physique
    - Vulnérabilité liée à la sécurité mémoire
- Patch disponible →
  - VMware ESXi 8.0 Update 3f
  - VMware ESXi 8.0 Update 2e
  - VMware Workstation Pro 17.6.4
  - VMware Fusion 13.6.4
  - VMware Tools 13.0.1.0

https://www.it-connect.fr/vmware-esxi-workstation-fusion-vulnerabilites-critiques-mars-2024/

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

Citrix NetScaler, patch corrigeant 3 vulnérabilités

CVE-2025-7775

- 0-day de type RCE liée à un dépassement de mémoire
  - Alerte de Citrix, faille exploitée par les attaquants
  - Vulnérabilité présente liée à une configuration spécifique pour Netscaler
    - Configuré en tant que Gateway ou serveur virtuel AAA
    - Utilise des serveurs virtuels de Load Balancing liés à des services IPv6
    - Utilise un serveur virtuel CR de type HDX
- Équipements concernés →
  - **NetScaler ADC** et **NetScaler Gateway 14.1** antérieures à la version **14.1-47.48**
  - **NetScaler ADC** et **NetScaler Gateway 13.1** antérieures à la version **13.1-59.22**
  - **NetScaler ADC 13.1-FIPS** et **NDcPP** antérieures à la version **13.1-37.241-FIPS** et **NDcPP**
  - **NetScaler ADC 12.1-FIPS** et **NDcPP** antérieures à la version **12.1-55.330-FIPS** et **NDcPP**
- Correction des vulnérabilités :
  - CVE-2025-7776 (DoS par dépassement de mémoire)
  - CVE-2025-8424 (problème de contrôle d'accès sur l'interface de gestion de NetScaler)

https://www.it-connect.fr/citrix-netscaler-cve-2025-7775-une-nouvelle-zero-day-exploitee-dans-des-attaques/

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

Vunérabilités sur SAP S/4HANA

CVE-2025-42957

- Injection de code ABAP dans un module exposé via RFC
  - Faisable via un compte utilisateur faible privilège
  - Permet de prendre le contrôle du système
  - Vidéo de présentation d'exploitation par Security Bridge : https://youtu.be/SNSaYb7ysmM
- Alerte de l'équipe de recherche sur l'exploitation active de la faille
- Patchs disponibles

- **S/4HANA (Private Cloud ou On-Premise)**, versions S4CORE 102 à 108.
- **Landscape Transformation (Analysis Platform)**, versions DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020.
- **Business One (SLD)**, versions B1_ON_HANA 10.0 et SAP-M-BO 10.0.
- **NetWeaver Application Server ABAP (BIC Document)**, versions S4COREOP 104 à 108, et plusieurs versions de SEM-BW.

https://www.it-connect.fr/sap-s4hana-cve-2025-42957-faille-critique-exploitee-cyberattaques/

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

Après BadSuccessor, c'est au tour de Golden dMSA

- Affecte une fonctionnalité introduite dans Windows Server 2025
- Accès à la clé racine KDS → permet de générer les MdP de tous les dMSA et gMSA
  - D'un domaine voire d'une forêt entière !
- Nécessite un accès préalable à la clé KDS racine
  - Implique déjà des privilèges très élevés : Root Domain Admins, Enterprise Admins, ou SYSTEM
  - Attaque intéressante à des fins de **persistance**
- Déroulé de l'attaque :
  1. Extraction de la clé KDS racine
  2. Énumération des comptes dMSA
  3. Calcul du paramètre << ManagedPasswordId >>
  4. Génération du mot de passe et obtention d'un ticket Kerberos AES256 valide
- Vulnérabilité principale :
  - Structure dMSA → 1.024 combinaisons seulement → brute-force rapide
  - Possibilité de contourner Credential Guard
- Mettre en place un audit SACL sur << msKds-RootKeyData >> !

https://www.semperis.com/blog/golden-dmsa-what-is-dmsa-authentication-bypass/

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

Faille 0-clic sur WhatsApp

CVE-2025-55177

- Présente sur les applications iOS et macOS
- Mauvaise gestion des autorisations
  - Lors de la synchronisation des appareils
  - Déclenchement de traitement du contenu d'une URL arbitraire
- Exploitation possible lorsqu'elle est enchaînée à la CVE-2025-43300
- Versions affectées :
  - WhatsApp pour iOS avant la version 2.25.21.73
  - WhatsApp Business pour iOS avant la version 2.25.21.78
  - WhatsApp pour Mac avant la version 2.25.21.78
- Notification en cours par WhatsApp

https://www.it-connect.fr/whatsapp-faille-zero-click-cve-2025-55177/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Une faille sur SharePoint qui coûte cher…

- Faille(s) en question :
  - **CVE-2025-53770** et **CVE-2025-53771**
    - 1 → RCE sans authentification grâce à une désérialisation non sécurisée
    - 2 → Path Traversal permettant une usurpation de compte + contournements de sécurité
    - Affectent les versions 2016, 2019 et Subscription Edition de SharePoint (on-prem)
    - Patchs disponibles
- Plus de 400 victimes, dont la NNSA
- Attaques menées par 3 groupes chinois
  - Linen Typhoon (APT27), Violet Typhoon (APT31) et Storm-2603
  - Scénario : compromission du SharePoint → chiffrement des données → demande de rançon

https://www.numerama.com/cyberguerre/2035745-plus-de-50-entreprises-piratees-a-cause-de-microsoft-sharepoint-et-ce-nest-pas-fini.html

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Sécurité de l'eSIM compromise

- Mise en lumière par une équipe de chercheurs polonais
  - 2 milliards de puces vulnérables
- Vulnérabilité dans l'application Java Card d'Oracle
- Clonage de profil eSIM
  - Possible de rediriger les appels et SMS (👋 Hello MFA)
  - Installation de backdoor dans les eSIM ou la désactiver
- Prérequis : disposer d'un accès physique pour installer Java Card et extraire les profils eSIM, des clés d'authentification OPc…
- Oracle déjà au courant depuis 2019
  - Réponse à l'époque : juste des « préoccupations de sécurité » qui n'affectent pas leur produit en production – FAUX
  - Patch distribué à des millions de puces… sachant qu'il y a 2 milliards de puces vulnérables…

https://korben.info/esim-vulnerabilite-clonage-kigen-security-explorations.html

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Contournement de Windows Defender

- Utilisation d'un pilote légitime, signé, mais vulnérable en bas niveau
  - Objectif : obtenir des droits élevés avec un logiciel vulnérable
  - Utilisation de la vulnérabilité pour désactiver Windows Defender
  - Puis installation d'un malware de haut niveau (comme Akira)

https://www.01net.com/actualites/microsoft-defender-vulnerable-des-pirates-trompent-lantivirus-windows-pour-deployer-le-ransomware-akira.html

Piratages, Malwares, spam, fraudes et DDoS
Piratage

WordPress et le plugin Gravity Forms

- Présence d'un fichier malveillant dans le dernier patch (*common.php*) du plugin
  - Récupération des informations URL, version de WordPress et de PHP, thèmes, plugins installés
  - Envoie vers le serveur de l'attaquant et réception de la charge utile
    - RCE sans authentification requise
    - Blocage des futures mise à jour
    - Ajout d'un compte admin WordPress caché
- Version vulnérable :
  - v2.9.11.1 et v2.9.12 en téléchargement direct
  - Via Composer entre 10 et 11 juillet
- Patch disponible → v2.9.13

https://www.01net.com/actualites/microsoft-defender-vulnerable-des-pirates-trompent-lantivirus-windows-pour-deployer-le-ransomware-akira.html

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Chess confirme une violation d'accès

- Déclaration officielle 3 mois après
- + 4.000/150.000 utilisateurs confirmés
- Accès non autorisé via une application de transfert de fichiers tierce
- Pas de mot de passe fuité → vigilance

https://hackread.com/chess-com-data-breach-3rd-party-file-transfer-tool/

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

Docker Hub héberge toujours des images Linux infectées par le backdoor XZ-Utils

- CVE-2024-3094 (cf. https://www.ossir.org/paris/supports/2024/2024-04-09/2024-04-09.pdf)
- 35 images Docker basées sur Debian (entre autres) signalées
  - Contiennent toujours cette backdoor
  - Mais pas que… les images de second niveau aussi (construites à partir de celles infectées)
- Debian a décidé de ne pas retirer les images
  - Jugées comme étant devenues des << artefacts historiques >>
    - Au risque d'exploitation faible
- Recommandations :
  - Ne pas utiliser d'images Docker obsolètes ou potentiellement compromises
  - Préférer les versions de xz-utils en 5.6.2 ou supérieures, exempte de la backdoor

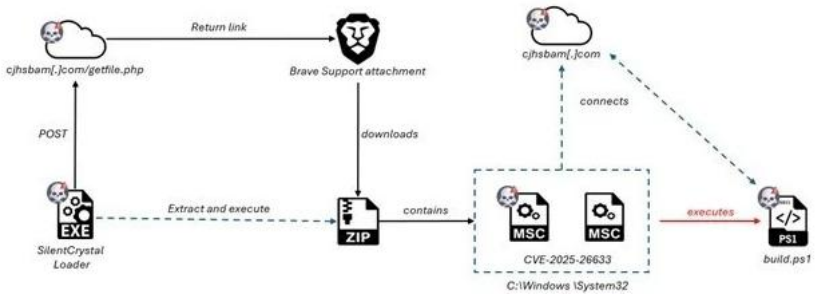
https://www.bleepingcomputer.com/news/security/docker-hub-still-hosts-dozens-of-linux-images-with-the-xz-backdoor/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Campagne de déploiement de l'infostealer Flick Stealer

- Réalisé par le groupe russe EncryptHub, mixte ingénierie sociale et exploitation technique
  - Prise de contact de la victime en tant que support pour prendre la main sur le poste de la victime
  - Installation de fichiers MSC via Powershell et installation
  - Établissement de la connexion vers le serveur C2 et récupération des infos de la victime
- Recommandation : bloquer l'IP 185.33.86[.]220

https://www.it-connect.fr/windows-encrypthub-exploite-la-faille-msc-eviltwin-pour-deployer-le-malware-fickle-stealer/



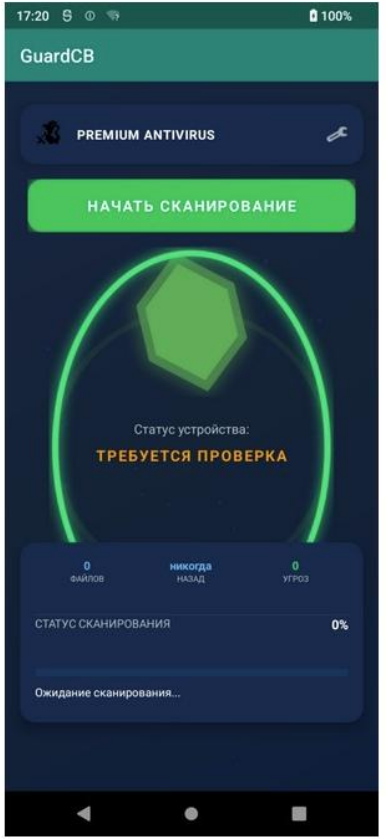
Source : Trustwave

Piratages, Malwares, spam, fraudes et DDoS
Malware

Android, le faux antivirus russe

- Malware en russe à destination des dirigeants russes
  - De son nom << Android.Backdoor.916.origin >>
  - Contient 2 leurres : GuardCB et SECURITY_FSB
  - Permet de faire des analyses antivirus avec 30% de chance de faux positifs
  - Demande l'autorisation d'accès à la géolocalisation, aux SMS, aux fichiers multimédias, à la caméra, au microphone…

https://www.it-connect.fr/ce-malware-pour-android-se-presente-comme-un-antivirus-developpe-par-le-fsb/



Source : Dr. Web

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

Mot de passe très faible chez McDonalds

- Système de recrutement par IA de McDonald's (McHire.com) piraté
  - Mot de passe utilisé (pour l'admin) : 123456
  - Et pour l'identifiant ? → 123456
- 30 minutes + 1x << Broken Access Control >> = compromission total de la plateforme
- Résultat ?
  - 64 millions d'enregistrements : noms, adresses mail, adresses postales, n° téléphone
  - Historique complet des conversations des **candidats** avec le recruteur IA
- Mise en place future d'un programme de bug bounty sur la plateforme

https://www.wired.com/story/mcdonalds-ai-hiring-chat-bot-paradoxai/

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

Après Free, SFR et Bouygues Telecom : Orange Belgium

- Intrusion détectée fin juillet 2025
- 850.000 comptes client compromis
  - Noms et prénoms des clients
  - N° téléphone
  - N° cartes SIM et codes PUK
  - Plans tarifaires associés
  - Aucun mot de passe, information financière ou adresse
- Tous les clients concernés ont reçu ou recevront une notification par SMS ou mail
  - Conseils donnés pour éviter des tentatives de phishing
- Orange France (Group) a également été victime fin juillet d'un piratage
  - Aucune exfiltration détectée

https://www.cysecurity.news/2025/08/orange-belgium-data-breach-exposes-850k.html

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

France Travail : +300.000 personnes concernées

- Communiqué officiel le 22 juillet 2025 sur un incident de sécurité sur le portail emploi pour les partenaires
- Organisme de formation Kairos responsable
  - Compromission d'un compte utilisateur par un infostealer
- Données pouvant contenir : nom, prénom, adresses postale et électronique, numéro de téléphone, identifiant France Travail et statut (inscrit, radié)

https://www.it-connect.fr/cyberattaque-france-travail-les-donnees-personnelles-de-340-000-personnes-exposees/

Piratages, Malwares, spam, fraudes et DDoS
Panne

Colt Telecom sous les projecteurs

- 12 août : panne de multiples services
  - Identifié initialement comme un simple problème technique
  - Service support affecté et non infrastructure client
- Revendication de l'attaque par Warlock et vente en ligne des informations
  - Échantillon de données comprenant des données financières, des employés, des clients et des dirigeants, des courriels internes et le développement de logiciels
  - Possiblement exploitation de la CVE-2025-53770 sur Sharepoint
- Toujours en cours d'investigation et de rétablissement

https://www.bleepingcomputer.com/news/security/colt-telecom-attack-claimed-by-warlock-ransomware-data-up-for-sale/?ref=veillecyber.fr

Piratages, Malwares, spam, fraudes et DDoS
Panne

Y a-t-il un pilote chez Aeroflot ?

- Attaque massive sur la compagnie aérienne russe
  - Revendiquée par des groupes d'hacktivistes ukrainien et biélorusse
  - Compromission d'un ensemble d'équipements : 122 hyperviseurs, 43 installations de virtualisation ZVIRT, une centaine d'interfaces de gestion de serveurs iLO et 4 clusters Proxmox
  - Phase finale : destruction de + 7.000 serveurs physiques/virtuels et postes de travail, 22 To de données au total
- Pas de confirmation d'intrusion, mais 60 vols annulés et beaucoup de retard
- Données exfiltrées avant destruction
  - Historique des vols, informations sur les postes de travail des employés, enregistrements d'appels téléphoniques et systèmes de surveillance du personnel
- Selon les hackers, un système de sécurité négligé et obsolète

https://www.it-connect.fr/la-compagnie-aerienne-russe-aeroflot-perturbee-par-une-cyberattaque-des-dizaines-de-vols-annules/

Piratages, Malwares, spam, fraudes et DDoS
Panne

Panne majeure – Crédit Mutuel, CIC, Monabanq

- A eu lieu le 30 août 2025 entre 17h20 et 19h30
- Dysfonctionnement interne des serveurs d'autorisation transactionnelle
- Conséquences :
  - Paiements et retraits impossibles
  - Millions de clients concernés
- 1ère panne d'une telle ampleur pour ce groupe de ~14 millions de clients

https://www.lefigaro.fr/conjoncture/une-panne-impacte-pendant-plus-de-deux-heures-des-milliers-de-clients-du-credit-mutuel-et-du-cic-20250830

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

Blue Team SadServers : améliorer ses performances Linux

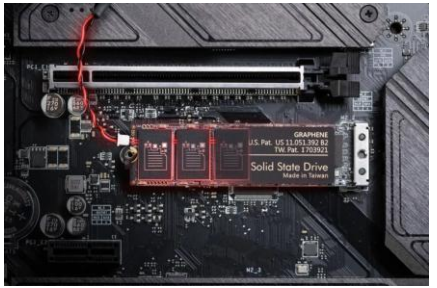
- Mise à disposition d'un ensemble de serveurs Linux
  - Différents scénarios
    - Gestion des services
    - Analyse de logs
    - Diagnostic de problèmes de connectivité, de permissions ou d'espace disque
    - Problèmes de performance
  - Pas d'installation à faire, connexion SSH vers les serveurs

https://sadservers.com/

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

P250Q : un SSD qui s'autodétruit #TeamGroup

- Circuit de destruction indépendant breveté (Taiwan Utility Model M662727 et US 12283335 B2)
- Deux modes d'effacement :
  - Effacement logiciel (S/W Quick Erase) : appui de 5 à 10s sur le bouton
    - Avec reprise automatique en cas de coupure d'alimentation
  - Effacement matériel (H/W Quick Erase) : appui de plus de 10s
    - Envoie une surtension qui détruit physiquement les puces NAND (fumée visible)
- Cibles : militaires, industriels - tous ceux qui manipulent des données ultra-sensibles
- Pas le premier du genre : https://www.tomshardware.com/news/SSD-RunCore-InVincible-self-destruct-NAND,15668.html
  - Produit qui a << disparu du marché >>
- Spécifications techniques :
  - Interface PCIe Gen 4×4, protocole NVMe 1.4
  - Jusqu'à 7 000 MB/s en lecture, 5 500 MB/s en écriture
  - Modèles 256 Go, 512 Go, 1 To et 2 To
  - Stable jusqu'à 105 °C



- Lauréat du 2025 Computex Best Choice Award, catégorie Cyber Security 🏆

https://korben.info/team-group-lance-p250q-ssd-autodetruit.html

Business et Politique

Business
Vie Privée

Mise à jour controversée des CGU de WeTransfer

- 06/25 : Mise à jour des CGU
  - Incluant le droit d'utiliser le contenu partagé pour entraîner ses modèles d'apprentissage automatique
  - Entrée en vigueur prévue le 8 août
  - Réaction : indignation massive → peurs, appels au boycott, alternatives mises en avant
- 07/25 : Rétractation
  - Nouvelle version des CGU publiée
  - Mention explicite à l'IA supprimée
  - WeTransfer affirme :
    - Ne pas utiliser les contenus pour entraîner des IA
    - Ne pas vendre ni partager les données avec des tiers

https://next.ink/brief_article/wetransfer-se-donne-lautorisation-dentrainer-des-ia-sur-les-contenus-quelle-heberge/

Business
Vie Privée

Fin de l’indexation des conversations ChatGPT par Google

- Été 2025 : option permettant aux utilisateurs de partager une conversation via un lien public
  - Expérimentation
  - Une case à cocher pour la rendre indexable par les moteurs de recherche
- GROS problème
  - Milliers de conversations avec du contenu sensible indexées
    - Conseils relationnels, sollicitations santé, candidatures, etc.
  - Jusqu’à 100.000 conversations selon 404 Media en lien avec l’enquête
- Suppression immédiate de la fonctionnalité le 31 juillet
  - OpenAI engage des actions pour faire retirer progressivement les contenus indexés

https://www.blogdumoderateur.com/chatgpt-abandonne-indexation-conversations-google/

Business
Monde

Apple envisage de racheter Mistral AI (et Perplexity)

- Rumeurs par Reuters sur le rachat des deux sociétés
  - Objectif : renforcer Siri et Apple Intelligence, combler le retard en IA
    - Et moindre dépendre de ses concurrents (👋Google et OpenAI)
  - Coût estimé : plusieurs milliards $ (valorisation Mistral > 6 Md$, Perplexity ~14 Md$)
- Positions internes chez Apple :
  - Eddy Cue (SVP Services) pousserait à l'acquisition
  - Craig Federighi (SVP Software Engineering) resterait favorable à un développement en interne
  - Rumeurs de partenariat/licence jugées plus réalistes à court terme
- Dernier grand deal d'Apple : Beats en 2014 (3 Md $)

https://intelligence-artificielle.developpez.com/actu/375164/Apple-aurait-envisage-d-acquerir-les-societes-d-IA-Mistral-AI-et-Perplexity-pour-accelerer-les-projets-d-Apple-en-matiere-d-IA-mais-l-acquisition-de-l-une-de-ces-entreprises-couterait-des-milliards-de/

Droit / Juridique / Politique
Monde

4 ans de prison pour ce développeur Java

- Histoire de Davis Lu : 55 ans, développeur depuis 2007 chez Eaton 🇺🇸
  - Rétrogradé en 2018
- Qu'a-t-il fait ?
  - Implantation d'un script Java sabotant les serveurs + kill switch (IsDLEnabledinAD)
  - Le 09 septembre 2019, c'est le drame ! (jour de son licenciement)
- Reconnu coupable en mai 2025
  - Couple de malveillance interne
  - 4 ans de prison ferme suivie de 3 ans de liberté surveillée

https://thehackernews.com/2025/08/ex-developer-jailed-four-years-for.html

Droit / Juridique / Politique
National

Le CNNum devient le Conseil de l'IA et du Numérique

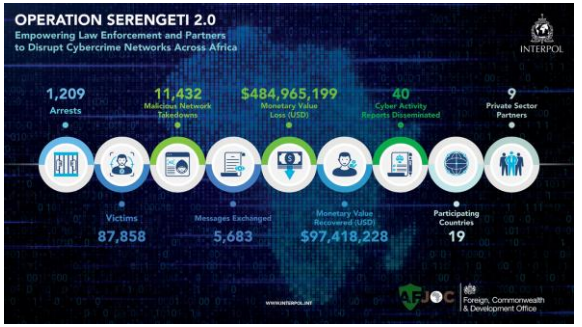
- Annoncé faite par la ministre déléguée Clara Chappaz
  - Transformation officialisée le 17 juin 2025 sur le site de la DGE
- Objectifs et mission du nouveau Conseil
  - Définir une stratégie claire pour le numérique et l'IA en France
  - Tenir compte des enjeux sociétaux, géopolitiques et numériques
- 14 personnalités qualifiées et parlementaires
  - Avec des groupes de travail thématiques incluant des experts associés selon les sujets
- Co-présidé par Anne Bouverot et Guillaume Poupard

https://www.entreprises.gouv.fr/la-dge/actualites/le-conseil-national-du-numerique-devient-le-conseil-national-de-lia-et-du

Opérations internationales

Opérations internationales
Opération

Opération Serengeti : arrestation de 1.209 cybercriminels



- Les chiffres parlent pour nous ---------->
- Opération qui a durée 3 mois (juin - août)
  - Acteurs : INTERPOL, 18 pays africains et le Royaume-Uni
  - But : lutter contre les crimes graves
    - Ransomwares, escroqueries en ligne et BEC
- Quelques faits marquants :
  - Angola : démantèlement de 25 centres de minage de cryptomonnaies
  - Zambie : démantèlement d'une énorme fraude en ligne à l'investissement crypto
  - Côte d'Ivoire : destruction d'une escroquerie à l'héritage initiée depuis l'Allemagne

https://thehackernews.com/2025/08/interpol-arrests-1209-cybercriminals.html

Conférences

Conférences

Passée(s)

- Black Hat USA, 02 au 07 août 2025 à Las Vegas
- DefCon, 07 au 10 août 2025 à Las Vegas
- Barbhack, 30 août 2025 à Toulon

À venir

- 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
- FIC, 14 au 15 Octobre 2025 au Canada

Divers / Trolls velus

Divers / Trolls velus

LLM 1-0 Test de Turing

- Information basée sur une étude sortie en mai 2025 (cf. arxiv)
- Comment s'est passé le test ?
  - En compétition : ELIZA, GPT-4 o, LLaMA-3.1-405B, et GPT-4.5
  - 2 tests randomisés, contrôlés et préenregistrés, avec des populations indépendantes
  - Chaque participant conversait 5 minutes simultanément avec un autre humain et avec un LLM
    - But : déterminer lequel était humain 🙋
- Résultats :
  - GPT-4.5 a été identifié comme humain 73% du temps 😱😱
  - LLaMA-3.1-405B comme humain 56% du temps 😱
  - GPT-4 o et ELIZA avec des taux bien en dessous du hasard, respectivement 21% et 23%

https://arxiv.org/abs/2503.23674

https://www.youtube.com/watch?v=OJWLZuaCO6I

Divers / Trolls velus

Suppression de l'OS Spoofing dans Tor Browser

- Fonctionnalité permettant de masquer l'OS utilisé
  - Au niveau du User-Agent (en-tête HTTP)
  - Objectif << anonymity set >>
- Supprimée = facilite le fingerprinting
- Bulletin du Tor Project de mai : `<< OS spoofing n'a jamais disparu >>`
  - Mais… les docs développeurs et les discussions sur GitLab confirment sa suppression
  - Accusations de << gaslighting >>
- Raison possible :
  - Trop coûteux de patcher Firefox ESR
  - Problème de compatibilité avec certains sites
  - Volonté de simplifier l'anonymity set
  - Hypothèse controversée : pression d'agences US (financeurs)

https://www.geeky-gadgets.com/tor-project-controversy-os-spoofing/

Divers / Trolls velus

Nouveau record de vitesse Internet

- Réalisé au Japon
  - Débit : 1.02 pétabit par seconde
  - Distance : 1.808 kilomètres
  - Type de fibre : 19 cœurs optiques (diamètre de gaine standard)
- Taille de Netflix en 2013 : 3.14 pétaoctets
  - 25 secondes pour tout télécharger

https://www.numerama.com/tech/2031323-tout-netflix-telecharge-en-une-seconde-que-se-passe-t-il-au-japon.html

Divers / Trolls velus

Piratage de Thermomix

- Mise en lumière de la vulnérabilité générale des équipements connectés du quotidien (domotique)
  - Travail réalisé par Synacktiv
- Mauvaise méthode chiffrement
  - Permet de tromper et de downgrade l'équipement
  - Pas de vérification d'intégrité, possible d'exécuter du code arbitraire (ex : en faire un point d'accès)
- Version vulnérable : v2.14
  - Admirable réaction de Vorwerk sur la transparence du rapport et la considération du problème

https://www.clubic.com/actualite-572874-des-experts-piratent-le-celebre-thermomix-et-devinez-quoi-son-fabricant-a-adore-l-initiative.html

Divers / Trolls velus

News sur Notepad++

- Rappel : vulnérabilité critique en juin découverte et patchée
  - Alerte de nombreux antivirus sur le patch
  - Raison : expiration du certificat de signature de code de notepad ++ (valide jusqu'à mai 2025)
  - Renouvellement échoué suite aux critères de validation et au rejet du nom de l'éditeur << Notepad++ >>
- Solution de gestion de la chaîne de certification en interne

https://www.it-connect.fr/notepad-plus-plus-cve-2025-49144-faille-windows/

Divers / Trolls velus

Encore un record battu pour CloudFlare

- Blocage d'une attaque DDoS avec un pic de 11.5 Tbps
  - Précédent record : 7.3 Tbps en juin
  - 360.000 musiques MP3 téléchargées en 1s
  - 1.400 films téléchargés en 1s

https://www.sdxcentral.com/news/cloudflare-blocks-massive-115-tbps-ddos-attack/

Divers / Trolls velus

Certificats TLS suspects émis pour 1.1.1.1 (CloudFlare)

- DNS (53/UDP) ou DoH (DNS-over-HTTPS)
- 3 certificats émis par une entreprise Croate (Fina)
  - Émis en mai 2025 par Fina RDC 2020
  - << Adversary-in-the-middle >> possible ; réel but inconnu
- Échec du Certificate Transparency
  - Conçu pour détecter et signaler rapidement des émissions frauduleuses
- Autorité absente des listes de Google, Mozilla et Apple

https://gbhackers.com/tls-certificate-mis-issuance-exposes-1-1-1-1-dns-service/

Divers / Trolls velus

Fausse alerte Google

- Rumeur invitant 2.5 milliards d'utilisateurs Gmail à changer leur mot de passe
  - Réponse de Google : NON
- Aucune faille de sécurité liée à Gmail et Google Workspace
  - Google rappelle que ses défenses bloquent plus de 99,9 % des phishings et des logiciels malveillants
- 2.5 milliards de comptes récupérés via un agrégat de fuites diverses

https://www.it-connect.fr/fausse-alerte-google-na-pas-demande-utilisateurs-gmail-de-changer-mot-de-passe/

Divers / Trolls velus

Word online par défaut

- Sauvegarde sur OneDrive
- Toujours possible de sélectionner un emplacement de stockage local
- Excel et PowerPoint, à venir dans l'année

https://www.it-connect.fr/windows-word-va-automatiquement-sauvegarder-vos-documents-dans-le-cloud-onedrive/

Divers / Trolls velus

Update licence pack d'extension Oracle VBox

- Mise à jour des conditions d'utilisation du pack d'extension
  - Renforcement sur l'utilisation uniquement personnelle du pack d'extension
- Audit d'Oracle pour vérifier son utilisation
  - << avec un préavis écrit de 45 jours, Oracle peut auditer votre utilisation du Produit pour confirmer que vous respectez les termes du présent Contrat >>
  - Action rétroactive si vous utilisez actuellement le pack pour une utilisation professionnelle

https://www.virtualbox.org/wiki/VirtualBox_PUEL

https://www.theregister.com/2025/07/30/licensing_change_oracle_virtualbox

FIN

Prochaine réunion ?

- RDV le **mardi 14 octobre 2025**

Accéder aux différents supports ?

Replays

Slides

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

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