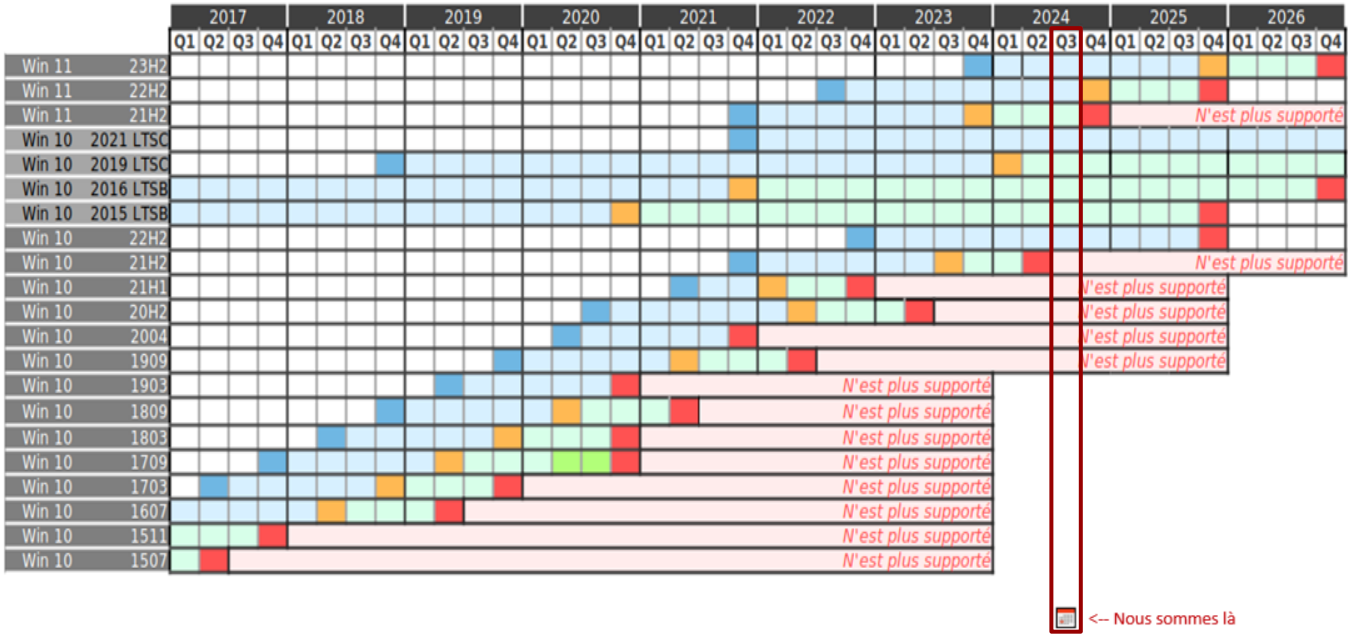
Revue d'actualité de l'OSSIR

10 septembre 2024

Jérémy De Cock
Melchior Courtois

Rappel du support Windows en couleurs

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



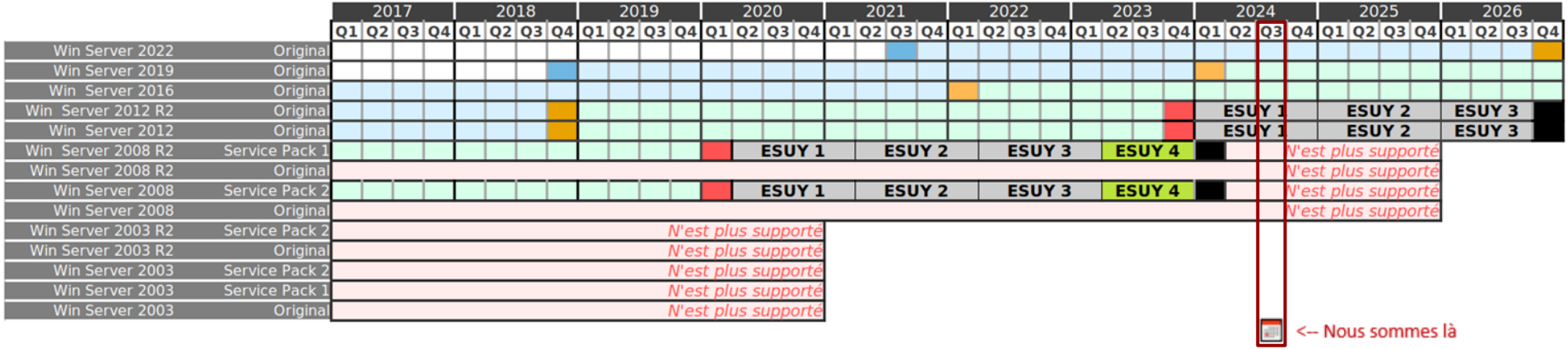
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



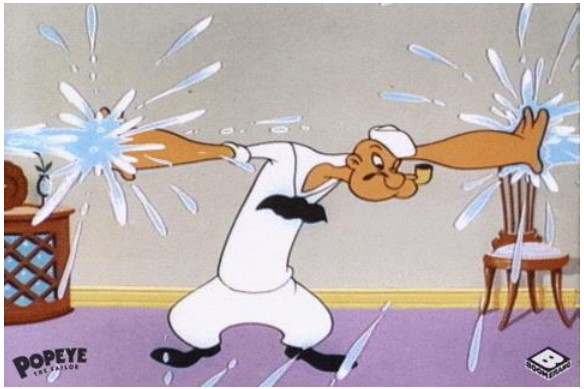
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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, 142 vulnérabilités patchées dont

- 4 vulnérabilités de type 0-day :
  - [**CVE-2024-38080**] Elévation de privilèges dans **Hyper-V**
    - Windows 11 et Windows Server 2022 sont les seules versions impactées
  - [**CVE-2024-38112**] Spoofing sur Windows **MSHTML**
  - [**CVE-2024-35264**] RCE dans .NET et Visual Studio
    - Entraînée par une race condition dû à un flux http/3 stoppé brutalement
    - Affecte .NET 8.0 et Visual Studio 2022 (versions 17.4, 17.6, 17.8 et 17.10)
  - [**CVE-2024-37985**] Aka FetchBench, leak de la mémoire sur des OS basés sur **ARM**
    - Tels que Windows 11 22H2 et 23H2
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2024-38053**] RCE sur Microsoft **SharePoint**
  - [**CVE-2024-38060**] RCE sur le **composant de gestion des images** de Windows
  - [**CVE-2024-38074,38076,38077**] RCE sur Windows **RDS**

https://www.it-connect.fr/microsoft-patch-tuesday-juillet-2024-142-failles-de-securite-et-4-zero-day/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de août, 89 vulnérabilités patchées dont

- 9 vulnérabilités de type 0-day :
  - [**CVE-2024-38178**] RCE 1-click sur le **moteur de script**
    - Nécessite l'utilisation de Edge en mode Internet Explorer
    - Windows 10 & 11 ainsi que Windows Server 2012 R2 à Windows Server 2022 impactés
  - [**CVE-2024-38193**] Use-after-free dans le **pilote de fonction auxiliaire pour WinSock**
    - Permet une élévation de privilèges (SYSTEM)
    - Windows 10 & 11 ainsi que Windows Server 2008 R2 à Windows Server 2022 impactés
  - [**CVE-2024-38213**] Bypass de **Mark of the Web** (encore)
    - Permet l'exécution de fichiers provenant d'Internet tout en ignorant le filtre SmartScreen
    - Windows 10 & 11 ainsi que Windows Server 2012 R2 à Windows Server 2022 impactés
  - [**CVE-2024-38106**] Elévation de privilèges dans le **noyau** Windows
    - Nécessite l'exploitation d'une race condition
    - Windows 10 & 11 ainsi que Windows Server 2016 à Windows Server 2022 impactés
  - [**CVE-2024-38107**] Elévation de privilèges dans **Power Dependency Coordinator**
    - Windows 10 & 11 ainsi que Windows Server 2012 R2 à Windows Server 2022 impactés
  - [**CVE-2024-38189**] RCE dans **Microsoft Project**
    - Nécessite la désactivation de la stratégie << Bloquer l'exécution des macros dans les fichiers Office provenant d'Internet >>
    - Microsoft Project 2016, Microsoft Office 2019, Microsoft Office 2021 LTSC et Microsoft 365 Apps for Enterprise impactés
  - [**CVE-2024-38199**] RCE dans **LDP**
    - Service déprécié par Microsoft qui n'est pas installé par défaut sur Windows
    - Windows 10 & 11 ainsi que Windows Server 2008 R2 à Windows Server 2022 impactés
  - [**CVE-2024-38200**] Leak de hash NTLM via un fichier distant ouvert depuis **Office**
    - Microsoft Office 2016, Microsoft Office 2019, Microsoft Office 2021 LTSC et Microsoft 365 Apps for Enterprise impactés
  - [**CVE-2024-21302**] Aka Windows Downdate, élévation de privilège via un downgrade de fichiers systèmes sur l'**OS**
    - Plus d'informations plus tard dans la présentation 😊

https://www.it-connect.fr/microsoft-patch-tuesday-aout-2024-89-failles-de-securite-et-9-zero-day/

Failles / Bulletins / Advisories
Systèmes

RCE 0-click unauthenticated dans la pile TCP/IP de Windows

CVE-2024-38063

- Patch fourni par Microsoft dans le patch Tuesday de juillet 2024
- Vulnérabilité présente dans la gestion du trafic IPv6
  - Integer Underflow
  - S’active avant que le FW ne gère le paquet !
- Affecte Windows 10 et 11 + toutes les éditions Windows Server entre 2008 et 2022
- Remédiation temporaire :
  - Désactiver IPv6 mais cela peut entraîner des dysfonctionnements !

https://securityonline.info/cve-2024-38063-cvss-9-8-0-click-rce-affects-all-windows-systems/

https://securityonline.info/windows-tcp-ip-vulnerability-cve-2024-38063-researchers-halt-exploit-release-due-to-severity/

Failles / Bulletins / Advisories
Systèmes

Plus d’infos sur Windows Downdate 💡

CVE-2024-38202 &
CVE-2024-21302

- Patch fourni par Microsoft dans le patch Tuesday de août 2024
- Vulnérabilités découvertes lors de la Black Hat 2024
  - Technique baptisée << Windows Downdate >> (nom également donné à l’outil des chercheurs)
- But : altérer Windows Update dans le but de réintroduire des vulnérabilités corrigées
  - Retrogradation de composants OS critiques : DLL, noyau NT, fonctionnalités telles que Credential Guard’s Secure Kernel et Hyper-V
  - Elévation de privilèges / exploits possibles et l’OS signale qu’il est entièrement à jour !

https://github.com/SafeBreach-Labs/WindowsDowndate (outil)

https://securityonline.info/poc-exploit-for-windows-0-day-flaws-cve-2024-38202-and-cve-2024-21302-released/

Failles / Bulletins / Advisories
Systèmes

Autre RCE 0-click sur Windows Server

CVE-2024-38077

- Patch fourni par Microsoft dans le patch Tuesday de juillet 2024
- Présente dans le service de licences Windows Remote Desktop
  - Baptisée << MadLicense >>
  - Service souvent présent où RDP est activé, outch
- Heap overflow dans la fonction << CDataCoding::DecodeData >>
  - Mauvaise gestion des entrées utilisateur
- Affecte toutes les Windows Server entre 2000 et 2025 !
  - 170k RDS exposés !

https://cybersecuritynews.com/madlicense-0-click-rce-flaw/

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Bug critique dans le gestionnaire de mot de passe de Chrome

- Disparition des mots de passe de 15 millions d'utilisateurs… 😱
  - … pendant 18 heures entre le 24 et 25 juillet
- Bug limité à la version M127 du navigateur Chrome sur Windows
- Une raison de plus pour ne plus stocker vos mots de passe sur votre navigateur 😊

https://securite.developpez.com/actu/360810/Google-s-excuse-apres-qu-un-bogue-dans-le-gestionnaire-de-mot-de-passe-de-Chrome-a-entraine-la-disparition-des-mots-de-passe-de-15-millions-d-utilisateurs-de-Windows-perturbant-leurs-flux-de-travail/#:~:text=Une%20estimation%20indique%20que%20le,sans%20garde%2Dfou%20appropri%C3%A9%22.

Failles / Bulletins / Advisories
Navigateurs (principales failles)

0.0.0.0 Day

- Rapport fait par Oligo le 7 août - vulnérabilité vieille de 18 ans
- Navigateurs vulnérables à l'adresse 0.0.0.0
  - Un site web public (comme les domaines .com, .fr, etc.) est capables de communiquer avec des services fonctionnant sur le réseau local (localhost) et potentiellement d'exécuter un code arbitraire sur l'hôte du visiteur en utilisant l'adresse 0.0.0.0 au lieu de localhost/127.0.0.1
- Windows non impacté par cette vulnérabilité
- Apple Safari, Google Chrome, Firefox en cours de déploiement d'un patch ou de solution préventive

https://www.oligo.security/blog/0-0-0-0-day-exploiting-localhost-apis-from-the-browser

Failles / Bulletins / Advisories
Navigateurs (principales failles)

9ème 0 Day pour Google Chrome

CVE-2024-7971

- Problème de confusion de type dans le moteur JavaScript V8
  - Peut permettre aux attaquants d'exécuter du code malveillant sur la victime, avec vol de données, l'accès non autorisé ou l'installation de logiciels malveillants
- Corrections de + 30 failles de sécurité avec le patch d'août
  - Passage en version 128
  - Version securisée de Chrome →
    - Les versions **128.0.6613.84/.85** pour **Windows/macOS**
    - La version **128.0.6613.84** pour **Linux**

https://securityonline.info/urgent-chrome-update-active-zero-day-exploit-detected-cve-2024-7971/

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

Hyperviseurs VMware ESXi intégrés à un AD

- Création automatique d'un groupe ESXi Admins lors de son intégration à l'AD
  - Accorde un accès administratif complet à l'hyperviseur ESXi
  - Pas de validation lors de l'ajout d'un utilisateur au groupe
  - Exploitation toujours possible si suppression puis recréation du groupe
- Selon un deuxième article, exploitation massive de cette faille
  - Version corrigée déjà en ligne depuis le 25 juin - VMware ESXi 8.0 U3

CVE-2024-37085

https://www.it-connect.fr/vmware-esxi-cve-2024-37085-cyberattaques-ransomwares-selon-microsoft/

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

Messagerie Exim : 1.5 millions de serveurs vulnérables

- 3.4 millions de serveurs Exim sur Internet
- Contourner les mécanismes de filtrage des pièces jointes
  - Mauvaise analyse de l'en-tête
  - Version vulnérable < v4.98

CVE-2024-39929

https://www.it-connect.fr/des-millions-serveurs-messagerie-exim-faille-de-securite-cve-2024-39929/

- 786 250 aux États-Unis
- 71 860 en Russie
- **69 440 au Canada**
- 64 830 au Pays-Bas
- **56 930 en France**
- 47 480 au Royaume-Uni
- 10 760 en Suède
- Etc.

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

RCE dans OpenSSH (again)


CVE-2024-6409

- Vulnérabilité présente dans le processus privsep
  - Race condition liée à la gestion des signaux
  - Privilèges réduits par rapport au processus parent (exploité par RegreSSHion)
- Affecte les versions 8.7p1 et 8.8p1 d'OpenSSH
  - Versions livrées avec Red Hat Entreprise Linux 9 !

https://www.it-connect.fr/linux-faille-de-securite-openssh-cve-2024-6409/

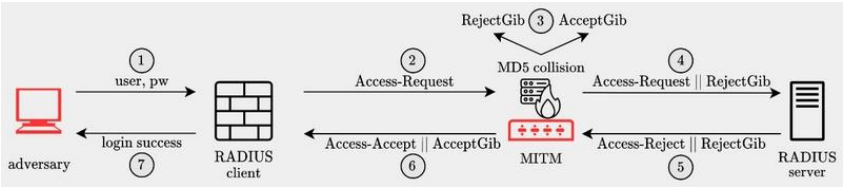
Failles / Bulletins / Advisories
Réseau (principales failles)

Nouvelle attaque sur le protocole RADIUS (CVE-2024-3596)

- Patch fourni par Microsoft dans le patch Tuesday de juillet 2024
- Surnommée Blast-RADIUS
  - Permet de contourner l'authentification AAA
  - Via une collision MD5 controlée ?
    - Utilisation de la fonction de hachage MD5 (**obsolète**)
  - Attaque nécessitant :
    - Entre 3 et 6 minutes > timeout des configurations RADIUS
    - Positionnement en MiTM
- Affecte toutes les implémentations du protocole
  - Utilisant une authentification non-EAP sur UDP !
- Utilisez RADSEC ou passez sur un serveur NPS (#Microsoft)

https://www.it-connect.fr/attaque-blast-radius-faille-de-securite-cve-2024-3596/

https://www.blastradius.fail/



Failles / Bulletins / Advisories
Smartphones (principales failles)

Android : Privesc sur le composant Android Framework

CVE-2024-32896

- Ancienne faille de juin 2024, censée affecter uniquement les Google Pixel
  - Google avait déployé un patch correctif pour cette vulnérabilité
  - Ce dernier confirme l'exploitation massive de cette vulnérabilité pour des attaques ciblées
- Prérequis d'exploitation : avoir un accès physique à l'équipement

https://www.it-connect.fr/android-mise-a-jour-de-septembre-cve-2024-32896/

Failles / Bulletins / Advisories
Autre (principales failles)

Temps difficile pour les Yubikeys

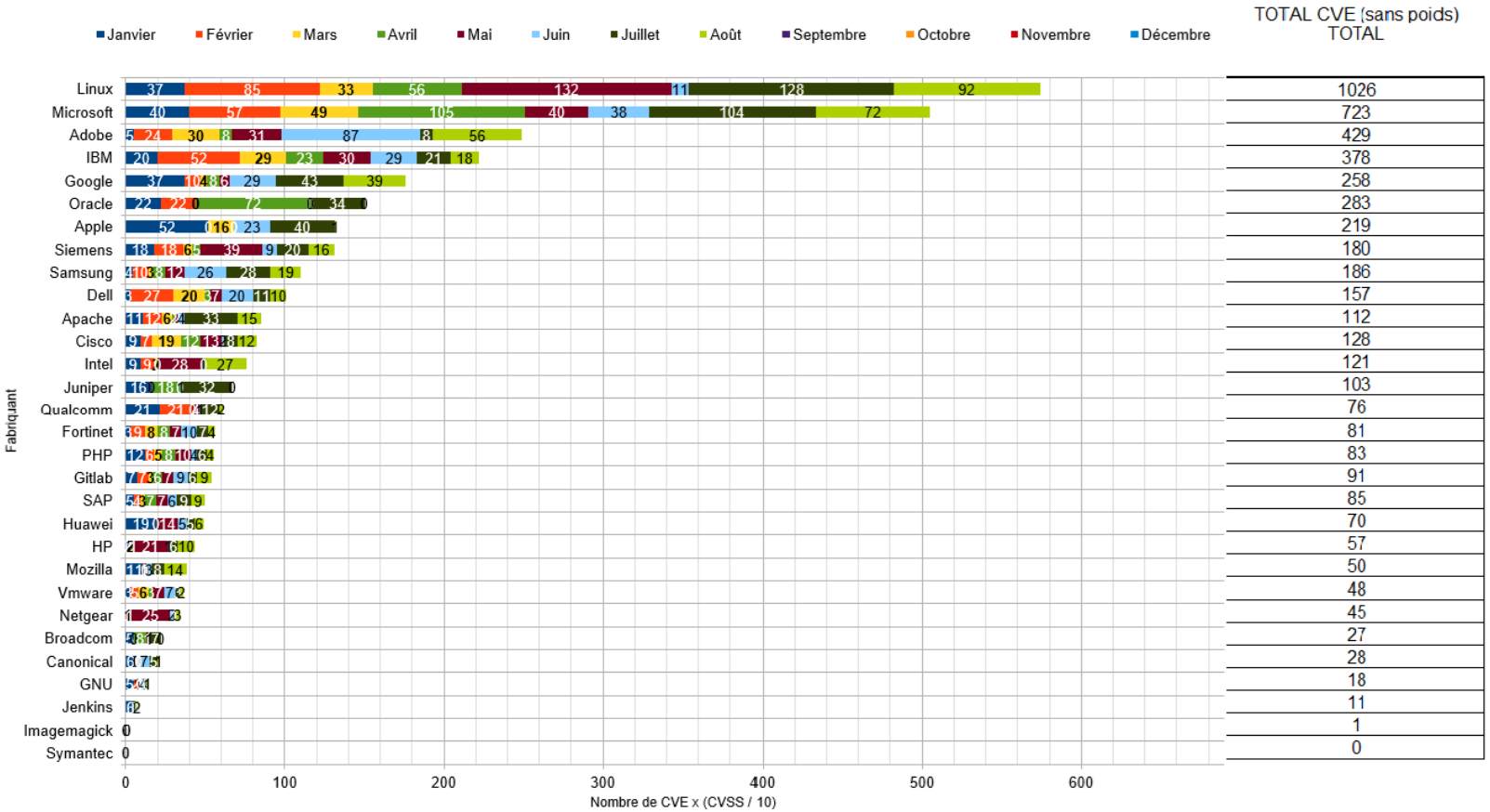
- << Side-channel attack >> nommée **Eucleak**
  - Permet à un attaquant de les cloner 😱
  - Facilitant la compromission des comptes protégés par la clé
- Vulnérabilité présente dans l'implémentation de ECDSA #Infineon
  - Trouvée par un chercheur de chez NinjaLab (cocorico)
- Si facile d'exploitation ?
  - Accès physique nécessaire
  - Excellentes connaissances en crypto et en électronique
  - Matériel spécialisé valant plus de 11k$
  - Réponse : non.
- Versions impactées ---------->
  - Impossible de mettre à jour le firmware…

- **YubiKey 5 Series** - Versions antérieures à 5.7
- **YubiKey 5 FIPS Series** - Versions antérieures à 5.7
- **YubiKey 5 CSPN Series** - Versions antérieures à 5.7
- **YubiKey Bio Series** - Versions antérieures à 5.7.2
- **Tous les produits de la série "Security Key"** - Versions antérieures à 5.7
- **YubiHSM 2** - Versions antérieures à 2.4.0
- **YubiHSM 2 FIPS** - Versions antérieures à 2.4.0

https://arstechnica.com/security/2024/09/yubikeys-are-vulnerable-to-cloning-attacks-thanks-to-newly-discovered-side-channel/

https://www.it-connect.fr/la-nouvelle-attaque-eucleak-permet-aux-pirates-de-cloner-les-cles-yubikey/

Failles / Bulletins / Advisories
Stats du mois



TOTAL CVE (sans poids) TOTAL
1026
723
429
378
258
283
219
180
186
157
112
128
121
103
76
81
83
91
85
70
57
50
48
45
27
28
18
11
1
0

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Capgemini, piratage venant d'un de ses consultants ?

- Victime du ransomware Knight en octobre 2023
  - Chiffrement des données concernant le travail pour un de ses clients
  - 5.000$ en Bitcoin demandé sinon → exfiltration (double extorsion)
- Non, c'est n'est pas un attaquant russe
  - Mais un consultant technique 🇫🇷 de la société depuis fin 2021
  - Actuellement en détention
- La rançon n'a pas été payée et aucune donnée ne semble avoir été volée

https://www.01net.com/actualites/firme-francaise-capgemini-piratee-employes.html

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Infiltré dans la société cyber américaine KnowBe4

- Hacker nord-coréen embauché en tant qu'ingénieur logiciel
  - 4 entretiens vidéo passés + vérifications d'usage ✅
  - Identité américaine volée + utilisation de photos provenant d'une banque d'images (IA 👋)
- Comment l'ont-ils débusqué ?
  - Il a installé un malware sur son ordinateur dès sa réception
  - Ce dernier a été automatiquement bloqué
  - La firme a contacté le FBI qui a pu découvrir la supercherie
    - L'ordinateur a été envoyé dans une << ferme >> d'ordinateurs aux US !

https://www.futura-sciences.com/tech/actualites/technologie-hacker-nord-coreen-fait-embaucher-comme-ingenieur-logiciel-entreprise-cybersecurite-americaine-114810/

https://eu.knoxnews.com/story/news/local/2024/05/16/fbi-raids-east-tennessee-laptop-farms-in-id-theft-scheme/73717532007/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Backdoor sur toutes les cartes MIFARE Classic ?

- Modèle FM11RF08S (société Fudan 🇨🇳)
  - Variante de la MIFARE qui n'est pas sous licence
  - Résiste aux attaques card only
  - Backdoor matérielle trouvée 😱
    - `<< This backdoor enables any entity with knowledge of it to compromise all user-defined keys on these cards without prior knowledge, simply by accessing the card for a few minutes. >>`
- Autres modèles de Fudan : backdoor similaire
- Vieilles cartes NXP et Infineon : aussi….
  - Production localisée en Chine 🧐
    - Coïncidence ?
- Bravo Quarkslab 👏🇫🇷

https://x.com/it4sec/status/1824770479363629170

https://blog.quarkslab.com/mifare-classic-static-encrypted-nonce-and-backdoors.html

https://www.linkedin.com/posts/fredraynal_backdoor-dans-les-cartes-mifare-activity-7231670300453539840-ybAr?utm_source=share&utm_medium=member_desktop

Piratages, Malwares, spam, fraudes et DDoS
Ransomwares

Rançon record : 75 000 000 $

- Entreprise du Fortune 50 ciblée par le groupe DarkAngels
  - Possiblement le géant pharmaceutique Censora
  - Cyberattaque subie en février 2024
  - Stratégie `<< Big Game Hunting >>` : peu de cibles mais cibles importantes

https://www.it-connect.fr/ransomware-dark-angels-une-entreprise-a-paye-une-rancon-record-de-75-millions-de-dollars/

Editeur de logiciel Octave victime de cyberattaque

- Ransomware le 16 août pour l'éditeur de logiciel Octave
  - Nombreux clients impactés : la Casserolerie, La Compagnie du Lit, Cash Piscines, Cultura, Lyophilisé & Co., Yvert & Tellier, Cobra, Agripartner, Kalico et TomPress
  - Réaction rapide et efficace des prestataires : isolation des serveurs compromis et mise en ligne d'un site de secours en -24h pour TomPress

https://france3-regions.francetvinfo.fr/occitanie/tarn/albi/cyberattaque-par-ransomware-des-grandes-marques-francaises-touchees-et-des-donnees-clients-compromises-3020933.html

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

1 To de données

- Partage d'un lien Mega sur Telegram d'une base de donnée issue de Telegram
  - Contient les informations de nombreuses entreprises : Adecco, Adobe, Badoo, La Poste Mobile, Catho, EuropeJobs, Service Postal, Deezer, Overblog…
  - Contient les numéros des cartes bleues associées aux utilisateurs
  - Mise à disposition gratuitement sur Telegram car aucun acheteur sur BreachForums

https://www.clubic.com/actualite-533160-nouvelle-fuite-massive-de-donnees-la-poste-mobile-adobe-deezer-et-adecco-touches-des-informations-sensibles-dans-la-nature.html

Marseille : vol de PC

- Vol d'une douzaine de PC dans les locaux d'Endel, prestataire de EDF
  - Contiennent des données sensibles sur les centrales nucléaires
  - Enquête ouverte afin de connaître les circonstances : préméditation, ciblage ?

https://www.lefigaro.fr/marseille/marseille-une-quinzaine-d-ordinateurs-contenant-des-donnees-sensibles-de-centrales-nucleaires-derobes-20240730

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

Fuite importante de données chez SFR

- 1.4 millions de données mise en vente sur << l'Amazon de la cybercriminalité >>
  - Base de données comportant 1.445.683 lignes
  - Noms, prénoms, n° de téléphone, adresses postales, dates de naissances…
- Puis les informations relatives à 50k abonnées
  - 2ème piratage (par des français) - French Hackers Squad

https://www.20minutes.fr/high-tech/4101644-20240716-sfr-donnees-1-5-million-clients-proposees-darknet-cybercriminel

https://www.it-connect.fr/50-000-abonnes-sfr-concernes-par-une-nouvelle-fuite-de-donnees-2024/

Base de données fuitée appartenant à ADT Inc.

- 30.812 enregistrements dont :
  - 30.400 courriels uniques
  - Adresses postales, IDs, produits achetés, etc.

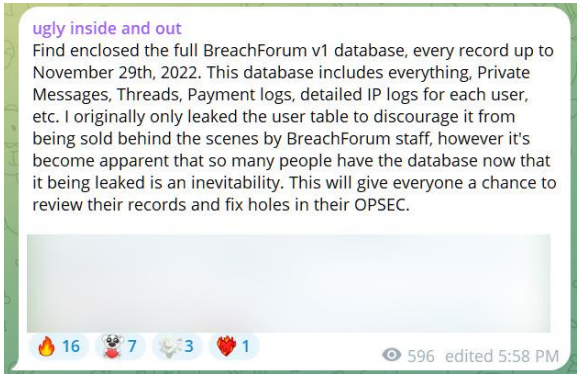
https://darkwebinformer.com/a-threat-actor-has-allegedly-leaked-a-database-belonging-to-adt/

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

Base de données ENTIÈRE de BreachForums V1 publiée gratuitement !

- Issue d'une sauvegarde vendue par Pompompurin (ancien gérant de la plateforme)
  - Vendue lors de sa liberté sous caution en juillet…
- Toutes les informations sur ses membres (< décembre 2022)
  - Noms, adresses mail, adresses IP, messages privés, adresses crypto, etc.
- L'acteur a l'origine de la fuite :
  - `<< Cela donnera à chacun une chance de revoir ses dossiers et de corriger les trous dans son OPSEC. >>`

https://www.bleepingcomputer.com/news/security/breachforums-v1-database-leak-is-an-opsec-test-for-hackers/



Piratages, Malwares, spam, fraudes et DDoS
Pannes

Sabotages de fibre pour 6 départements

- Dans la nuit du 28 juillet, sabotage du câble longue distance de SFR
  - 6 départements touchés : Bouches-du-Rhône, l'Aude, l'Oise, l'Hérault, la Meuse et la Drôme
  - Ralentissement du réseau mais non interruption car passage par des chemins de secours
  - 2 jours avant : incendie criminel près de Toulouse sur les équipements réseaux avec revendication par un site local d'ultragauche

https://www.lemonde.fr/pixels/article/2024/07/29/de-reseaux-de-fibres-optiques-de-plusieurs-operateurs-victimes-de-sabotages-nocturnes-dans-six-departements_6260956_4408996.html

Piratages, Malwares, spam, fraudes et DDoS
Pannes

DDoS massif sur des applications cloud Azure

- Erreur dans les mécanismes de protection automatisés de Microsoft ?
  - Azure Front Door (AFD) et Azure Content Delivery Network (CDN) pas au top
- Plusieurs entreprises impactées à travers le monde
  - Azure DevOps (ADO), Azure Virtual Desktop (AVD), services LinkedIn et Microsoft 365 impactés
  - Ex : Starbucks avec sa commande mobile désactivée pendant plusieurs heures

https://azure.status.microsoft/en-gb/status/history/ (rapport post-incident de Microsoft)

https://www.clubic.com/actualite-534084-microsoft-cible-par-une-attaque-ddos-qui-a-declenche-une-reaction-inattendue-de-ses-systemes-de-defense.html

Piratages, Malwares, spam, fraudes et DDoS
Pannes

La GROSSE affaire CrowdStrike

- Version 7.11 de son EDR Falcon = 💥
  - MAJ diffusée le vendredi 19 juillet 2024 entre 04h09 UTC et 05h27 UTC (78 minutes)
  - Plusieurs millions de machines impactées à travers le monde
- BSoD sur les machines, même après reboot !
  - Dû à un << out-of-bonds memory read >>
  - Crash de composants critiques de l'OS
- Pertes estimées à plusieurs milliards (selon quelques assurances)
  - Aéroports, hôpitaux, grandes surfaces, etc. impactés
- Remédiation simple mais pénible (surtout si le disque est chiffré)
  - Du côté de CrowdStrike : amélioration des tests de validation !

https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

https://www.crowdstrike.com/blog/falcon-update-for-windows-hosts-technical-details/

https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

https://www.reuters.com/technology/fortune-500-firms-see-54-bln-crowdstrike-losses-says-insurer-parametrix-2024-07-24/

https://news.microsoft.com/2009/12/16/microsoft-statement-on-european-commission-decision/

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Panne électrique chez Global

- Message d'Octave Klaba sur Linkedin le 5 août indiquant une panne dans le DC Global Switch
  - Cause technique, non malveillante selon les vérifications
  - Panne de 3H
  - Impact sur l'AP-HP (Assistance publique-Hôpitaux de Paris)

https://dcmag.fr/une-panne-electrique-dans-un-datacenter-parisien-de-global-switch/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Rapport annuel de cybersécurité du COMCYBER-MI

- Fait un état des lieux des défis de 2023 en matière de cybersécurité
  - Lutte contre les cybercriminels
  - Techniques utilisées
  - Evolutions juridiques
  - Prévisions futures

https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024

Piratages, Malwares, spam, fraudes et DDoS
Publication

APT-29 fournie par NSO et Intellexa ?

- Hypothèse émise suite à un rapport de Google's TAG
  - Dans le cadre d'attaques sur des sites web du gouvernement mongol
- TTPs similaires avec d'autres entités
  - NSO : exploit pour la CVE-2024-5274 sur Chrome
  - Intellexa : payload pour la CVE-2023-41993 sur iOS
- Comment ont-ils récupéré ces exploits n-day ?

https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

Piratages, Malwares, spam, fraudes et DDoS
Publication

DirectAccess -> Always On VPN

- Suppression de DirectAccess de Windows pour les prochaines versions
- Passage avec Always On VPN
  - Plus flexible, plus sécurisé et prise en charge du MFA
  - Permet de prendre en charge des machines IN et OUT AD
  - Lien de migration disponible pour la transition sur le site de Microsoft : https://learn.microsoft.com/en-us/windows-server/remote/remote-access/da-always-on-vpn-migration/da-always-on-migration-overview?WT.mc_id=AZ-MVP-5004580

https://www.it-connect.fr/windows-directaccess-est-obsolete-vous-devez-migrer-vers-always-on-vpn/

Business et Politique

Business
Monde

Apple VS Patreon

- Exigences d'Apple de passer par l'achat intégré d'iOS pour les dons et le système de paiement pour Patreon -> commission de 30%
  - Passage des plans de facturation au premier mois ou à la création à la facturation par abonnement
  - Mise en conformité limite pour l'ensemble des créateurs de la plateforme - novembre 2025
  - Sinon Menace de retirer l'application de l'App Store
- Tim Sweeney a recommandé de passer par la version web ou l'application Android pour effectuer les achats afin de ne pas avoir la commission d'Apple

https://ios.developpez.com/actu/361424/Apple-exige-une-commission-de-30-pourcent-sur-tous-les-dons-aux-createurs-via-Patreon-et-menace-de-retirer-l-application-de-l-App-Store-si-elle-n-adopte-pas-le-systeme-d-achat-integre-d-iOS/

Bienvenue à LIDL dans le secteur du cloud

- Développement depuis 2 ans avec une mise en service en interne
  - Proposer un service cloud en accord avec la réglementation européenne
  - Concurrencer les acteurs Big Tech (Google, Amazon, Microsoft) sur le contrôle des données

https://www.francetvinfo.fr/internet/amazon/lidl-veut-s-emanciper-des-geants-du-numerique-en-developpant-ses-propres-outils-de-cloud_6751366.html

Business
National

Thales : gel des recrutements d'ingénieurs français

- Note du 10 juillet indiquant une priorisation des recrutements en Inde et en Roumanie au sein de leur centre de compétence d'ingénieries
  - Cependant Thales rétorque avec 2 000/12 000 postes ouverts en France
  - Service impacté : R&D, service client et management des offres
  - Le Royaume-Uni est aussi concerné par ce gel
- Complication sur le long par rapport à la sincérité de Thalès

https://allegro-informatique.fr/allegro-informatique-fr-8868-thales-met-un-terme-a-ses-recrutements-dingenieurs-en-france-et-au-royaume-uni

Levée de fonds de 11M€ en série A pour Patrowl ! 👏🇫🇷

- But : intensifier la conquête du marché européen et la R&D
- Levée menée (principalement) par Crédit Mutuel Innovation

https://www.patrowl.io/blog-levee-de-fond-2024/

Droit / Juridique / Politique
Monde

Le début de la fin pour Telegram ?

- Pavel Durov, son PDG franco-russe, interpellé à l'aéroport du Bourget (France)
  - Faisait l'objet d'un mandat de recherche français
    - Pour cause des nombreuses dérives de Telegram (blanchiment d'argent, trafic de stupéfiants, etc.)
    - Manque de modération de sa part
  - Et d'une plainte en Suisse (aussi) pour violence sur un de ses enfants
- Mis en examen le 28 août et sous contrôle judiciaire (caution de 5M€)
- Mouvements << Free Pavel >> et << Free Durov >> créés
  - Des opérations lancées contre la France allant du DDoS à la faille SQL
- Quelles sont les suites pour Telegram ? Fin des messageries chiffrées ?
  - Pendant que d'autres parlent de la fin de la liberté d'expression en Europe (hein Musk)

https://www.bfmtv.com/police-justice/le-pdg-franco-russe-de-la-messagerie-cryptee-telegram-interpelle-en-france_AN-202408240359.html

https://www.zataz.com/free-durov-la-resistance-numerique-au-bon-gout-du-marketing/

https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf

https://www.lemonde.fr/pixels/article/2024/09/02/en-coree-du-sud-la-police-ouvre-une-enquete-contre-telegram-pour-diffusion-de-deepfakes-pornographiques-impliquant-des-mineurs_6302041_4408996.html

Droit / Juridique / Politique
Monde

Condamnation de Sellafield

- Défaillance de cybersécurité sur + 75% des serveurs du site nucléaire
  - Détail du rapport : `<< Possible de télécharger et d'exécuter des fichiers malveillants sur les réseaux informatiques de Sellafield's IT via une attaque de phishing sans déclencher d'alarmes >>`
  - Multiples problèmes : série de défaillances informatiques à l'entreprise publique datant de plusieurs années, contamination radioactive et la culture toxique sur le lieu de travail
  - Plus de 4 ans d'inaction en terme de cybersécurité

https://www.theguardian.com/business/article/2024/aug/08/sellafield-apologises-guilty-plea-security-failings-nuclear

Conférences

Conférences

Passée(s)

- **Barbhack**, 31 août 2024 à Toulon
- **Black Hat USA**, 03 au 08 août 2024 à Las Vegas
- **DefCon**, 12 au 13 août 2024 à Las Vegas
- **DefCon Paris**, 9 septembre 2024 à Paris

À venir

- **FranSec**, 10 septembre 2024 à Paris
- **Les Assises**, 09 au 12 octobre 2024 à Monaco
- **Hexacon**, 04 au 05 octobre 2024 à Paris

Divers / Trolls velus

Divers / Trolls velus

Suicide de robot en Corée du Sud

- Robot municipale aidant les habitants dans les tâches administratives
  - Retrouvé inerte le jeudi 20 juin à 16H
  - Enquête ouverte afin de comprendre les raisons, possiblement un suicide lié à une grosse charge de travail (9h à 18h)

https://www.leparisien.fr/high-tech/il-etait-lun-des-notres-un-robot-fonctionnaire-se-suicide-en-coree-du-sud-en-se-jetant-dun-escalier-26-06-2024-D6GWNOIWMNAONEOKPX64RJJCZU.php

800 millions d'heures de travail gratuites

- Rapport de la part de chercheurs (on ne sait pas lesquels) sur l'exploitation des humains afin de résoudre les CAPTCHA Google
  - Sur 13 ans, plus de 800 millions d'heure perdus - environ 6,1 milliards de dollars
  - Serve à entraîner gratuitement les IA de Google à la résolution de CAPTCHA
  - Fausse sécurité : GPT-4 a réussi à contourner ce test anti-robot en faisant croire qu'il était une personne souffrant d'une déficience visuelle à un employé qui a alors résolu le captcha à sa place

https://www.bfmtv.com/tech/google/comment-google-a-fait-travailler-les-internautes-gratuitement-pendant-800-millions-d-heures_AV-202407240523.html

Divers / Trolls velus

Le génie de Waterloo : futur ingénieur nucléaire

- Construction d'un réacteur à fusion dans sa chambre d'étudiant
  - Importation des composants depuis Internet
  - Utilisation de l'IA Claude 3.5 d'Anthropic comme assistant
  - Moyen financiers : 2000 €

https://www.mobeez.fr/actualites/13869/avec-2000-euros-et-un-ordinateur-cet-etudiant-cree-un-reacteur-a-fusion-dans-sa-chambre-et-atteint-le-plasma-defiant-les-geants-de-lenergie-et-leurs-milliards/

Une affaire qui aurait pu coûter cher

- Tentative d'escroquerie d'un employé licencié du New Jersay avec menace de suppression des sauvegardes, interruption de 254 serveurs et désactivation des comptes admin
  - Enquête du FBI suite à la demande de rançon et découverte d'une connexion frauduleuse récente
  - Création de tâches planifiés modifiant les mots de passe administrateurs locaux et utilisateurs
  - Démasqué par l'historique de navigation web d'une VM

https://www.it-connect.fr/un-homme-bloque-acces-254-serveurs-extorquer-des-fonds-a-son-ancien-employeur/

FIN

Prochaine réunion ?

- RDV le **mardi 15 octobre 2024**

Accéder aux différents supports ?

Replays

Slides

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

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