Revue d'actualité de l'OSSIR

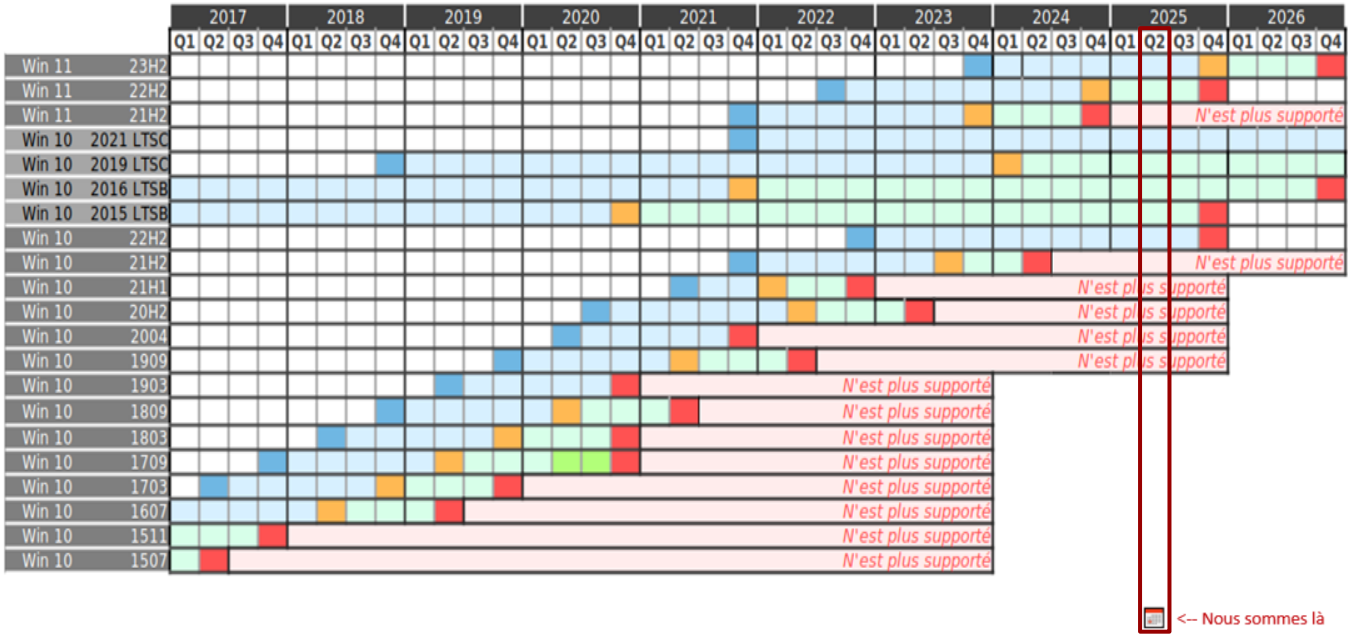
08 avril 2025

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***



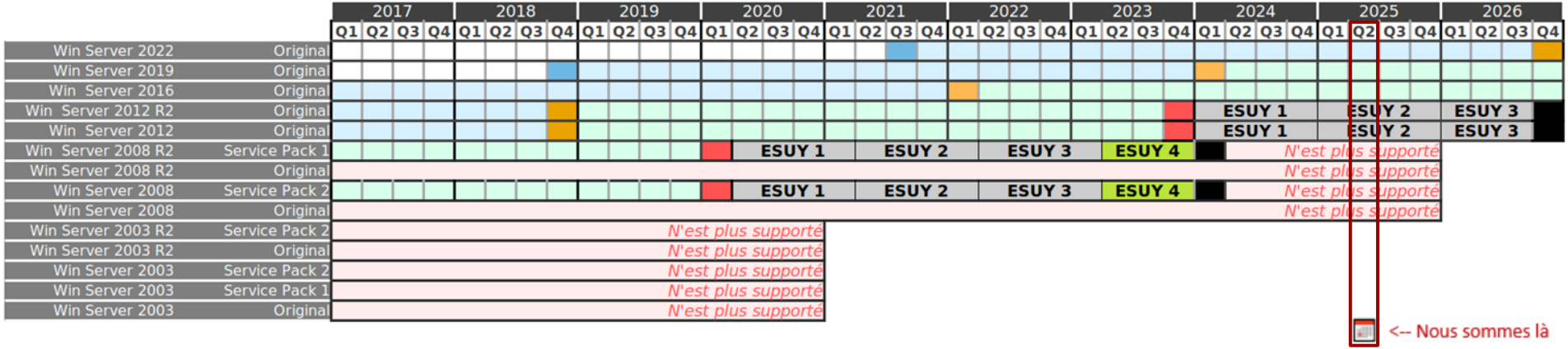
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



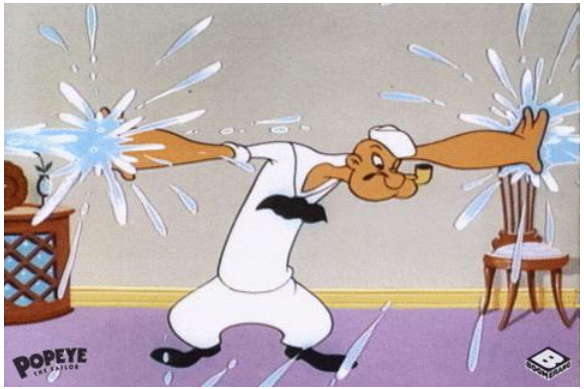
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 février, 55 vulnérabilités patchées dont

- 4 vulnérabilités de type 0-day :
  - [**CVE-2025-21391**] Elévation de privilèges, Windows Storage
    - << Limitée >> puisqu'elle ne permettrait << que >> du supprimer des fichiers ciblés (#DoS)
    - Affecte Windows 10 & 11 et Windows Server ≥ 2016
  - [**CVE-2025-21418**] Elévation de privilèges, pilote Ancillary Function (WinSock)
    - Permet d'obtenir les privilèges SYSTEM
  - [**CVE-2025-21194**] Bypass de l'UEFI, Microsoft Surface
    - Cible les machines virtuelles au sein d'un hôte UEFI
    - Affecte Surface Hub, Surface Pro 8, Surface Pro 9, Surface Go 2, Surface Laptop 3, etc.
  - [**CVE-2025-21377**] Leak et manipulation de hash NTLM, protocole NTLM
    - Nécessite une interaction utilisateur sur un fichier (peu importe l'action)
    - Affecte Windows 10 & 11 et Windows Server ≥ 2008
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2025-21177**] RCE, Microsoft Dynamics 365 Sales
  - [**CVE-2025-21381**] RCE, Microsoft Office - Excel
  - [**CVE-2025-21379**] RCE, service DHCP de Windows Server

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

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de mars, 57 vulnérabilités patchées dont

- 7 vulnérabilités de type 0-day :
  - [**CVE-2025-24983**] Elévation de privilèges, sous-système du noyau Windows (Win32)
    - Permet d'obtenir les privilèges SYSTEM via une race condition (locale)
    - Affecte Windows 10 et Windows Server ≤ 2016
  - [**CVE-2025-24984**] Memory disclosure (via heap), Windows NTFS
    - Nécessite un périphérique USB (physique)
  - [**CVE-2025-24985**] RCE, Windows Fast FAT
    - RCE, mais l'attaque doit être menée << localement >> (??)
    - Nécessite le montage d'un VHD malveillant
  - [**CVE-2025-24991**] RCE, Windows NTFS
    - //
  - [**CVE-2025-24993**] RCE, Windows NTFS
    - Type << Heap-based overflow >>
  - [**CVE-2025-26633**] RCE, Microsoft Management Console
    - Nécessite, à priori, une interaction utilisateur avec un fichier ".msc"
  - [**CVE-2025-26630**] RCE, Microsoft Access
    - Affecte Microsoft Office 2016, 2019, 2021, 2024 et Microsoft 365 Apps for Enterprise

Affecte Windows 10 & 11 et tous les Windows Server

https://www.it-connect.fr/patch-tuesday-mars-2025-microsoft-a-corrige-57-vulnerabilites-dont-7-failles-zero-day/

Failles / Bulletins / Advisories
Système

FortiOS Authentication Bypass


CVE-2025-24472

- Affecte FortiOS et FortiProxy
- Permet à un attaquant d'obtenir des accès super-admin
  - Via des requêtes CSF proxy
- Risques ?
  - Création de faux comptes admin
  - Modification des politiques de pare-feu
  - Accès aux VPN SSL
- Versions impactées ?
  - Versions **FortiOS** 7.0.0 à 7.0.16
  - Versions **FortiProxy** 7.0.0 à 7.0.19
  - Versions **FortiProxy** 7.2.0 à 7.2.12
- Patchez et/ou désactivez l'accès au panel admin (au moins filtrez)

https://cybersecuritynews.com/cisa-fortinet-fortios-authentication/

Failles / Bulletins / Advisories
Système

PAN-OS Authentication Bypass


CVE-2025-0108

- Affecte PAN-OS
- Permet à un attaquant non authentifié d'invoquer certains scripts PHP
  - `<< While invoking these PHP scripts does not enable remote code execution, it can negatively impact integrity and confidentiality of PAN-OS >>`
- Versions impactées ?
  - PAN-OS 11.2 : versions antérieures à 11.2.4-h4
  - PAN-OS 11.1 : versions antérieures à 11.1.6-h1
  - PAN-OS 10.2 : versions antérieures à 10.2.13-h3
  - PAN-OS 10.1 : versions antérieures à 10.1.14-h9
- Patchez et/ou désactivez l'accès au panel admin (au moins filtrez)

https://www.helpnetsecurity.com/2025/02/13/pan-os-authentication-bypass-palo-alto-networks-poc-cve-2025-0108/

Failles / Bulletins / Advisories
Système

VMware : CVE importantes

CVE-2025-22224
CVE-2025-22225
CVE-2025-22226

- 3 CVE
  - Heap-overflow vulnerability, arbitrary write vulnerability and information-disclosure vulnerability
  - Permet d’échapper à une machine virtuelle invitée et obtenir le contrôle total de l'hyperviseur et du système hôte
  - Affectent VMware ESXi, vSphere, Workstation, Fusion, Cloud Foundation et Telco Cloud Platform
- Prérequis : être administrateur de la machine invité

https://www.theregister.com/2025/03/04/vmware_plugs_three_hypervisorhijack_holes

Failles / Bulletins / Advisories
Système

Hyperviseur Windows Hyper-V


CVE-2025-21333

- 0-day permettant une privEsc
  - Heap-overflow : exploitation du pilote vkrnlintvsp.sys, surcharge dans l'entrée du tampon I/O Ring pour obtenir des capacités de lecture/écriture arbitraires dans le noyau Windows
- PoC publié et vulnérabilité déjà exploitée par les groupes de hackers
- Faille présente et testée dans Windows 11 23H2, fortement possible sur la 24H2 (last) mais aussi sur Windows Server

https://www.it-connect.fr/hyper-v-un-exploit-poc-a-ete-publie-pour-cette-vulnerabilite-exploitee-comme-zero-day/

Failles / Bulletins / Advisories
Système

PrivEsc sur le kernel Linux


CVE-2025-0927

- Heap-overflow sur les systèmes Ubuntu 22.04
  - Risque : DoS et execution de code
  - Prérequis : pouvoir monter un système de fichiers, normalement limité aux processus CAP_SYS_ADMIN
  - Contournement possible avec les versions Desktop et Server avec des règles de polkit par défaut

https://securityonline.info/cve-2025-0927-public-exploit-released-for-linux-kernel-privilege-escalation-bug/

Failles / Bulletins / Advisories
Système

Faille critique sur Ivanti Connect Secure


CVE-2025-22457

- Type << Stack-based buffer overflow >>
  - Exploitable à distance !
  - Ni authentification, ni interaction utilisateur requisent
- Solution Ivanti Connect Secure patchée (22.7R2.6), mais pas les autres :
  - Pulse Connect Secure (Obsolète) : 22.7R2.6 (contactez Ivanti)
  - Ivanti Policy Secure : 22.7R1.4 (disponible le 21 avril 2025)
  - ZTA Gateways : 22.8R2.2 (disponible le 19 avril 2025)
- Exploitée par UNC5221 (groupe chinois)
  - Utilisée pour déployer les malwares Dryhook et Phasejam
- Réinitialisez l'appliance avant de la monter de version !

https://www.it-connect.fr/des-cyberespions-chinois-exploitent-cette-nouvelle-faille-dans-les-solutions-ivanti-cve-2025-22457/

Failles / Bulletins / Advisories
Navigateur (principales failles)

0-day fortement exploitée sur Chrome


CVE-2025-2783

- Pas réellement d'information technique sur la faille
- Permet de contourner la sandbox de Chrome
  - Ce qui permet ensuite d'infecter les clients
  - Affecte uniquement Chrome sur Windows
- Exploitée dans la campagne de cyberespionnage ForumTroll
  - Cible les russes ?
- Passez sur la version 134.0.6998.178 (ou supérieur)

https://www.bleepingcomputer.com/news/security/google-fixes-chrome-zero-day-exploited-in-espionage-campaign/

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

Google : 2 vulnérabilités corrigées

- Permettent d'exposer les adresses mails des comptes Youtube
  - Utilisation de l'ID Gaia, identifiant pouvant être partagé entre les services Google
  - Permet de révéler l'adresse mail associée
- Découvertes en septembre 2024 et patchées en février 2025
  - Récompense de 13.000 $ pour les chercheurs

https://www.bleepingcomputer.com/news/security/google-fixes-flaw-that-could-unmask-youtube-users-email-addresses/

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

9 failles de sécurité sur GLPI 10.0.0.18

- 3 failles critiques !
  - [**CVE-2025-24799**] Injection SQL non authentifiée via le point de terminaison de l'inventaire
  - [**CVE-2025-24801**] RCE authenticated
  - [**CVE-2025-21619**] Injection SQL via la configuration des règles
- Injections SQL possible grâce à la fonction handleAgent située dans */src/Agent.php*
  - Rapport détaillée : https://blog.lexfo.fr/glpi-sql-to-rce.html
- 700 serveurs GLPI (potentiellement) vulnérables en France (source : ONYPHE)
  - 3.000 au niveau mondial
  - Important de noter que la fonctionnalité d'inventaire doit être activée !

https://www.it-connect.fr/patchez-glpi-plus-de-3-000-serveurs-sont-vulnerables-a-ces-deux-failles-importantes/

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

RCE via WinZip

CVE-2025-1240

- Validation insuffisante des données fournies par l'utilisateur
  - Plus précisement lors de l'analyse de fichier 7z
- Type << Out-of-bounds Write >>
  - Nécessite la visite d'une page malveillante ou l'ouverture d'un fichier malveillant
- Passez sur la version 29.0 de WinZip !

https://securityonline.info/cve-2025-1240-winzip-vulnerability-opens-door-to-remote-code-execution/

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

RCE sur Wazuh Server (le SIEM du moment)

CVE-2025-24016

- Désérialisation non sécurisée permettant une RCE
  - Cible `as_wazuh_object` (plusieurs moyens d'y arriver)
  - Nécessite un accès à l'API de Wazuh (coucou les agents 👋)
- Affecte uniquement la version 4.9.0 (sortie en décembre 2024)

https://github.com/wazuh/wazuh/security/advisories/GHSA-hcrc-79hj-m3qh (rapport + PoC disponible)

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

Vulnérabilité dans l'outil interactif PostgreSQL (psql)


CVE-2025-1094

- Injection SQL → exécution de code arbitraire (ACE)
  - Mauvaise gestion des caractères UTF-8 invalides
- Découverte lors de l'enquêtes sur la CVE-2024-12356
  - RCE dans les logiciels BeyondTrust (décembre 2024)
- Passez sur les versions suivantes :
  - PostgreSQL 17 → 17.3
  - PostgreSQL 16 → 16.7
  - PostgreSQL 15 → 15.11
  - PostgreSQL 14 → 14.16
  - PostgreSQL 13 → 13.19

https://thehackernews.com/2025/02/postgresql-vulnerability-exploited.html

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

RCE sur Apache

CVE-2025-24813

- Publié en mars 2025, repose sur un stockage de session par fichiers
  - Configuration répandue
- Exploitation en 2 étapes
  - Envoi d'une requête PUT contenant une charge utile Java sérialisée et encodée en base64, stockée en tant que fichier de session sur le serveur Tomcat
  - Envoi d’une requête GET avec un cookie JSESSIONID pointant vers ce fichier de session, ce qui force Tomcat à le désérialiser et à exécuter le code malveillant.
- Patch disponible, sinon
  - Revenir à la configuration par défaut du servlet (readonly="true")
  - Désactiver la prise en charge des requêtes PUT partielles
  - Éviter le stockage de fichiers sensibles dans un sous-répertoire d'un répertoire public

https://www.it-connect.fr/apache-tomcat-cette-faille-activement-exploitee-seulement-30-heures-apres-sa-divulgation-patchez/

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

0-click sur Whatsapp

- Critique, permet d'installer un logiciel espion sur équipement
  - Déploiement en masse du malware Graphite
  - Contourne les protections Android, accédant ainsi à d'autres applications, y compris des messageries chiffrées
- Pas de CVE attribuée
  - Pression politique et économique ?

https://www.zataz.com/une-faille-0-click-dans-whatsapp-exploitee-pour-installer-le-logiciel-espion-graphite/

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

Failles OpenSSH pour clients et serveurs

CVE-2025-26465
CVE-2025-26466

- MiTM
  - Prérequis : option *VerifyHostKeyDNS* activée (“yes” et “ask”)
  - Possible d’intercepter une session SSH, accédant à des données sensibles, ou même pivoter vers d'autres systèmes critiques du réseau
- Déni de service lors de la pré-authentification
  - Détectable par une consommation anormale de CPU et de mémoire
  - Atténuation possible avec les paramètres : *ConnexionGraceTime*, *MaxStartups*, et *PerSourcePenalties*
- Patch disponible → v9.9p2

https://securityonline.info/openssh-flaws-cve-2025-26465-cve-2025-26466-expose-clients-and-servers-to-attacks/

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

Mise à jour de OpenVPN

CVE-2025-2704

- Risque de DoS des serveurs VPN (concerne uniquement les serveurs)
  - Prérequis : option *--tls-crypt-v2* active
  - Malformation des paquets avec l'instruction ASSERT()
- Patch disponible → v2.6.14
  - Sinon possible de désactiver l'option

https://www.it-connect.fr/patchez-openvpn-cette-nouvelle-faille-de-securite-peut-faire-planter-votre-serveur-vpn/

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

Rapport de Qualys, sécurité Ubuntu compromise

- Contournement des restrictions des utilisateurs
  - Possible de créer des espaces de noms d'utilisateurs avec des capabilities admin
  - Mise en évidence des techniques de contournement : via aa-exec, via busybox, via LD_PRELOAD
- Mesures de protection possibles et recommandées :
  - Activer *kernel.apparmor_restrict_unprivileged_unconfined=1* pour bloquer l'abus d'aa-exec
  - Restreindre les profils AppArmor permissifs pour BusyBox et Nautilus
  - Appliquer un profil AppArmor plus strict à Bubblewrap (bwrap) pour les applications utilisant les espaces de noms utilisateur
  - Utiliser aa-status pour identifier et désactiver les profils à risque

https://www.it-connect.fr/securite-ubuntu-menacee-par-ces-faiblesses-des-actions-manuelles-sont-requises/

Failles / Bulletins / Advisories
Smartphone (principales failles)

Patch Google corrigeant 44 vulnérabilités Android

- [**CVE-2024-43093**] Elévation de privilèges, composant Framework
  - Permet un accès non autorisé aux répertoires *Android/data*, *Android/obb* et *Android/sandbox*
    - Ainsi qu'à leurs sous-répertoires
- [**CVE-2024-50302**] Fuite de mémoire, composant HID USB (noyau)
  - Fuite (locale) via des rapports HID
- Correctifs fournis (comme d'habitude) aux fabricants

https://www.it-connect.fr/android-google-corrige-44-vulnerabilites-avec-le-patch-de-mars-2025/

Failles / Bulletins / Advisories
Smartphone (principales failles)

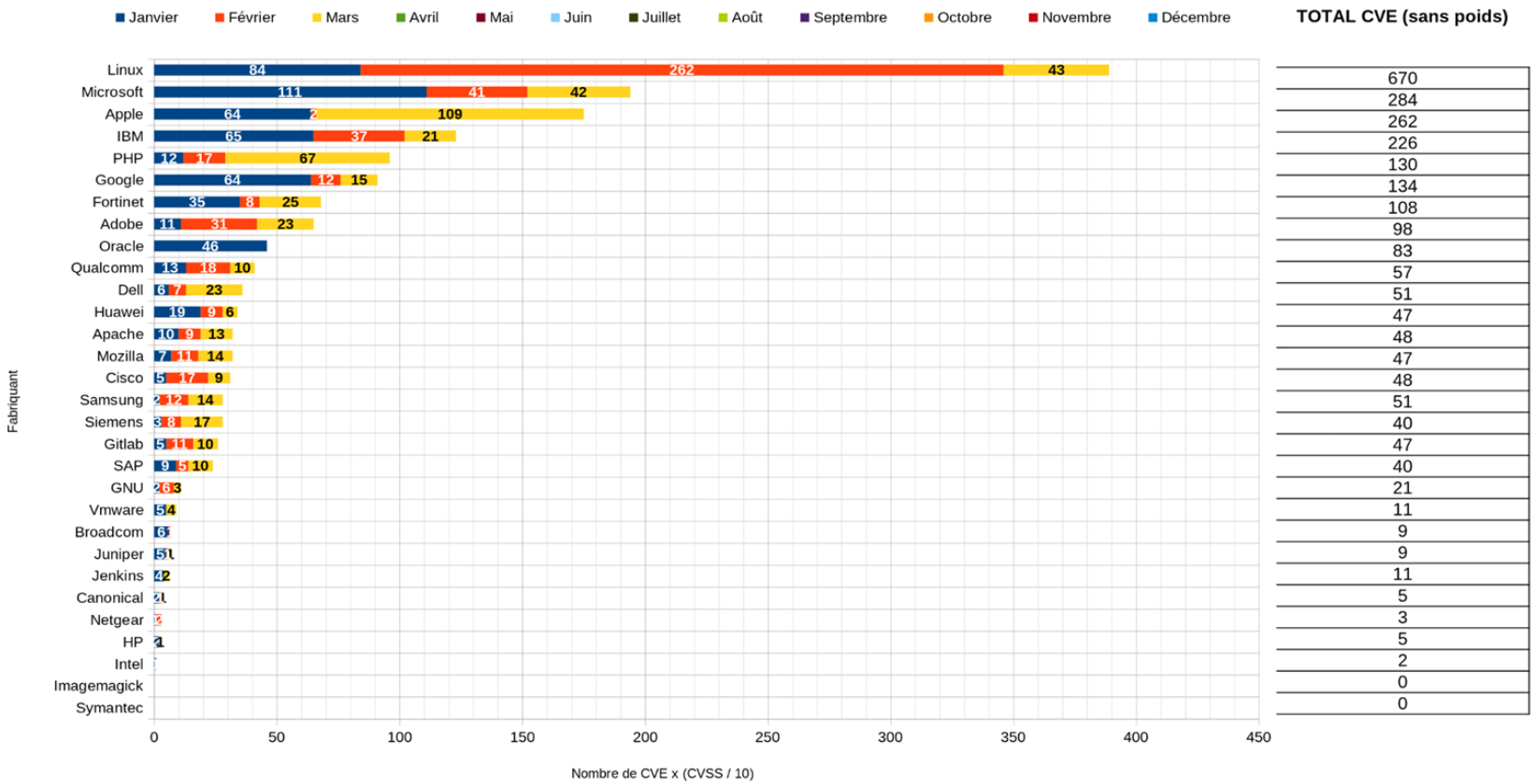
Contournement du mode restreint USB d'Apple

CVE-2025-24200

- Fonctionnalité permettant de verrouiller le port USB après 1h d'inactivité pour les équipements Apple
- PoC disponible avec analyse et debug du code

https://blog.quarkslab.com/first-analysis-of-apples-usb-restricted-mode-bypass-cve-2025-24200.html

Failles / Bulletins / Advisories
Stats du mois



Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Paralysie du secteur financier : Harvest

- Fintech 🇫🇷 leader de logiciels financiers
  - Outil de gestion de patrimoine, CRM, etc.
- Attaque par un de ses fournisseurs
  - Victime d'un ransomware (à l'origine)
- Impacts ?
  - Activités de banques, sociétés de gestion et de patrimoine paralysées (pendant 3 semaines)
  - Données personnelles de clients comme MAIF et BPCE exposées
- Renforcez la sécurité des chaînes d'approvisionnement et surveillez vos prestataires !
  - Wait… DORA ?

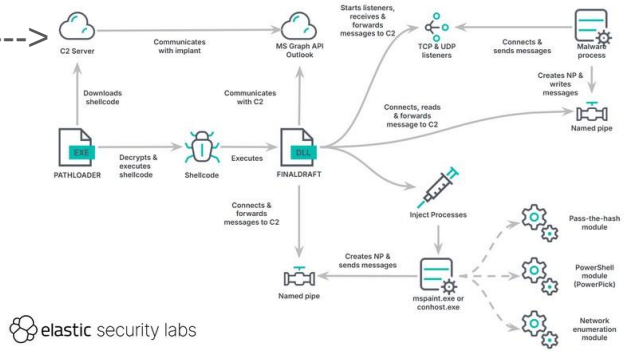
https://www.lefigaro.fr/societes/fuite-de-donnees-paralysie-du-secteur-financier-ce-qu-il-faut-savoir-sur-la-cyberattaque-contre-harvest-20250324

Piratages, Malwares, spam, fraudes et DDoS
Malware

FinalDraft : malware original

- Infection via **PathLoader** (executable malveillant)
  - But : télécharger le malware FinalDraft
- Communication grâce à des mails en brouillon
  - Via l'API Microsoft Graph #Outlook
  - Token demandé à https://login.microsoftonline.com/common/oauth2/token
    - Trafic vu comme légitime
  - Envoie et reçoit des ordres par l'intermédiaire des brouillons ------->
- Variante compatible avec Linux
- Cas d'attaques observées :
  - Ministère des Affaires étrangères d'un pays d'Amérique du Sud
  - Tentatives en Asie du Sud-Est

https://www.elastic.co/security-labs/finaldraft



Piratages, Malwares, spam, fraudes et DDoS
Malware

Android TV : victime du botnet Vo1d

- + 1.5 millions d'appareils compromis dans + 200 pays
  - Pic d'activité le 14 janvier avec + 800.000 bots
- Fonctionne comme proxy, contournement géographique, dissimulation d'attaque
- 3 principaux pays touchés : Brésil, Afrique du sud, Indonésie
- Situation qui peut évoluer très vite
  - En 3 jours, croissance de 4.900% (4.000 → 200.000) en Inde

https://www.it-connect.fr/le-botnet-vo1d-a-infecte-plus-de-15-million-dappareils-android-tv-dans-226-pays/

Piratages, Malwares, spam, fraudes et DDoS
Ransomware

Ransomware Ghost 👻

- Déjà compromis des organisations de plus de 70 pays
  - Surtout des critiques !
  - Alerte du CISA et du FBI
- Anciens noms : Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada et Rapture
- Pas d’attaques ciblées mais plutôt opportunistes :
  - Serveur exposé + vulnérabilité connue pas patchée
- Vulnérabilités exploitées :
  - Fortinet : CVE-2018-13379
  - ColdFusion : CVE-2010-2861, CVE-2009-3960
  - Microsoft Exchange : CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (ProxyShell)

https://www.bleepingcomputer.com/news/security/cisa-and-fbi-ghost-ransomware-breached-orgs-in-70-countries/

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

Caisse des dépôts : identifiants compromis

- Base de données fuitée avec 70.000 utilisateurs
  - Contient les noms, prénoms, date et lieux de naissance, numéro de sécurité sociale et adresse
  - Pas de coordonnées bancaires, ni téléphoniques
  - Communication réalisée rapidement auprès des personnes concernées

https://www.usine-digitale.fr/article/une-cyberattaque-vise-la-caisse-des-depots-les-donnees-de-70-000-personnes-subtilisees.N2227416

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

Piratage chez Chronopost → Fuite de données

- Incident survenu le 29 janvier
  - Vol du nom, prénom, adresse, numéro de téléphone ainsi que la signature des clients du service de livraison par le cybercriminel
  - Entrainant une campagne de phishing

https://www.numerama.com/cyberguerre/1903243-chronopost-victime-dun-piratage-massif-des-millions-de-donnees-clients-en-danger.html

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

Chasse aux Tesla (ça va trop loin)

- Publication des données personnelles des propriétaires 🇺🇸 de TESLA
  - Fait suite aux tensions contre MUSK et sa société
  - Données : noms, adresses postales, adresses électroniques et numéros de téléphone
- But : pousser les propriétaires de TESLA à vendre leurs véhicules
  - Si vous voulez que le propriétaire du site supprime vos données

https://www.numerama.com/cyberguerre/1929201-chasse-aux-tesla-un-site-seme-la-panique-en-publiant-les-donnees-personnelles-des-proprietaires.html

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

Fuite de données chez Orange

- Comprenant des milliers de documents internes
  - Incluant des enregistrements d'utilisateurs et des données d'employés
    - Mais aussi des adresses électroniques, code source, factures, contrats, etc.
    - ~ 6.5 Go
  - Concerne la branche roumaine de l'entreprise
- L'intrusion a, à priori, été réalisée sur une application non critique
  - Rey, membre du groupe HellCat, a l'origine de cette fuite de données
- Une rançon a été demandée mais Orange n'a pas entamé de négociations

https://www.bleepingcomputer.com/news/security/orange-group-confirms-breach-after-hacker-leaks-company-documents/

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

Base de données non protégée et en libre accès

- Contient des milliards de mots de passe Wi-Fi et des adresses IP
  - ~ 2.7 milliards d'enregistrements - 1.17 To
  - Mais aussi des SSID, des n° identification d'appareils, etc.
- Les données appartiendraient à LG-LED SOLUTIONS LIMITED

https://www.it-connect.fr/une-base-de-donnees-non-protegee-expose-des-milliards-de-mots-de-passe-wi-fi-et-des-adresses-ip/

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

Oracle Cloud : mensonge sur le piratage

- Compromission d'un serveur Oracle
  - `<< Il n'y a pas eu de violation d'Oracle Cloud. Les informations d'identification publiées ne concernent pas Oracle Cloud. Aucun client n'a été victime d'une violation ou n'a perdu de données. >>`
  - Informations validées par certains utilisateurs
  - 6 millions d'informations volées pouvant contenir des mots de passe SSO et LDAP
  - Sujet à suivre

https://www.lemondeinformatique.fr/actualites/lire-des-clients-confirment-la-fuite-de-donnees-oracle-cloud-96454.html

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Panne chez Whatsapp et Messenger

- 28 février : impact mondiale
  - Messenger : ralentissement du service
  - Whatsapp : réception et envoie de message impossible, ni appel vocaux
- Bug technique avec correction en quelques heures
  - Impact sur les utilisateurs, les communications professionnelles et l'utilisation d'autre plateforme comme Signal et Telegram

https://www.capital.fr/economie-politique/whatsapp-et-messenger-en-rade-un-enorme-bug-frappe-meta-1509863?trk=public_post_comment-text

Business et Politique

Business
Vie Privée

Google autorise le fingerprinting à ses annonceurs

- Permettant d'identifier votre appareil avant même que vous ayez accepté des cookies !
  - Adresse IP + infos sur votre navigateur + infos sur votre OS + fuseau horaire + … = votre empreinte
- GROS enjeux de confidentialité
  - Quasi impossible à détecter ou à bloquer
  - Violation du RGPD et de la directive ePrivacy selon W3C et l'EFF
- `<< plus de liberté aux partenaires quant à la façon dont ils ciblent les annonces et mesurent leurs performances >> #Google`
- Téléviseurs connectés, consoles de jeu, enceintes intelligentes, etc. également concernées

https://www.blogdumoderateur.com/google-autorise-fingerprinting-dangers-donnees-personnelles/

Business
Vie Privée

Siri un peu trop à l'écoute

- Signalement et plainte déposée par LDH au parquet de Paris contre Apple
  - Visant la collecte massive d'enregistrements de Siri
  - S'appuient sur les signalements fournis par un ancien employé (lanceur d'alerte)
    - Il a écouté des heures d'enregistrements (~ 1300 enregistrements / jour)
- Enregistrements collectés à l'insu des utilisateurs (entre 2014 et 2024)
  - Conversations intimes, politiques, relations sexuelles…
- Apple a accepté de payer 95 millions de $
  - 20 $ par appareil aux consommateurs lésés (aux USA uniquement)
  - Et confirme que les données n'ont jamais été vendues
- Système d'apprentissage de Siri retravaillé

https://www.lemonde.fr/pixels/article/2025/02/14/conversations-enregistrees-par-siri-apple-vise-par-un-signalement-et-une-plainte-en-france_6546033_4408996.html

Business
Nationale

Nouveau président pour le campus Cyber

- Joffrey Célestin-Urbain reprend les rênes
  - Ancien salarié au ministère de l'Économie, des Finances et de l'Industrie, puis au ministère de l’écologie
  - 2018 : chef du Service de l'information stratégique et de la sécurité économiques (SISSE) à la Direction générale des Entreprises

https://www.linkedin.com/posts/vincent-strubel-7b7056200_nomination-du-futur-pr%C3%A9sident-du-campus-cyber-activity-7310192744058994690-eRc1?rcm=ACoAABfYHo0BiCBb5qdB1zQWL8DZKwBfAXdSaDQ

Business
Monde

Attention à la dépendance

- Changement de stratégie pour les entreprises américaines
  - Fonctionnalités gratuites pour des logiciels ou applications → payantes
  - Exemple avec Starlink : dépendance de l'Ukraine pour résister à la Russie
- Souveraineté : sujet controversé
- Appel à essayer de créer en France pour réduire cette dépendance

https://www.lexpress.fr/economie/high-tech/lukraine-privee-de-starlink-quand-donald-trump-montre-le-vrai-prix-de-la-tech-americaine-AIXAHVXLKNCF3GT74B6BO4VZE4/?cmp_redirect?cmp_redirect=true

Business
Monde

Russie : mise en conformité logiciel

- Obligation de Poutine d'abolire l'utilisation des logiciels occidentaux par les entreprises
  - Annonce le 12 juin avec effet le 1er janvier
  - Secteur concernés : agricole, automobile et énergie
- Réalité : transition difficile
  - Utilisation de logiciels occidentaux pour beaucoup d'entreprises (Microsoft, Google…)

https://www.geo.fr/geopolitique/la-deche-a-moscou-la-substitution-des-logiciels-occidentaux-par-des-alternatives-nationales-en-russie-defi-impossible-223497

Business
Monde

Baisse du niveau de sécurité des données sur l' << iCloud britannique >> par Apple

- Les autorités 🇬🇧 ont demandé à Apple d'insérer une backdoor sur les iPhone & Mac
- Apple a refusé
  - … et a décidé de désactiver la protection avancée des données (ADP) sur iCloud
  - Fonctionnalité permettant de chiffrer les sauvegardes iCloud
- La mesure prise n'impacte pas :
  - Le gestionnaire de mots de passe, les données de santé et les logiciels de conversation
- Pour les utilisateurs ayant activé ADP disposent d'un délai pour la désactiver

https://www.bfmtv.com/tech/apple/apple-va-mettre-fin-au-chiffrement-des-donnees-sur-le-cloud-au-royaume-uni_AD-202502210637.html?at_brand=BFMTV&at_compte=BFMTV&at_plateforme=twitter

Business
Monde

Google veut (toujours) acheter Wiz

- Acquisition pour 32 milliards de $
  - L’achat devrait se finaliser pour fin 2026
- Pourquoi acheter ?
  - Wiz compte plus de 45% des sociétés figurant au classement Fortune 100 dans ses clients
  - But visé : renforcer la position de Google sur le marché de la sécurité informatique
- Rachat historique pour Google
  - Record précédent correspondant à celui de Motorola Mobility pour 12.5 milliards de $ en 2012
- À voir si la FTC est du même avis…

https://www.lemonde.fr/pixels/article/2025/03/18/cybersecurite-google-va-racheter-wiz-pour-plus-de-29-milliards-d-euros_6583299_4408996.html

Business
Monde

IBM rachète Hashicorp

- Acquisition pour 6.4 milliards de $
- Continuité dans la stratégie des vastes investissements d'IBM dans les logiciels d'automatisation pour aider les organisations à optimiser leurs dépenses en IT et à réduire leurs coûts
- Inclut :
  - Un logiciel alimenté par l'IA pour les informations de gestion des applications dans les portefeuilles des clients afin d'identifier
  - Un logiciel pour une observabilité complète de la pile IT
  - Des outils de gestion des ressources applicatives
  - Des solutions de gestion financière
  - Un logiciel pour intégrer des milliers d'applications et de données dans des environnements de cloud hybride

https://newsroom.ibm.com/2025-02-27-ibm-completes-acquisition-of-hashicorp,-creates-comprehensive,-end-to-end-hybrid-cloud-platform

Droit / Juridique / Politique
National

Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

- But : transposer / intégrer 3 textes européens
  - La directive sur la résilience des entités critiques (REC)
  - La directive Network and Information Security (NIS 2)
  - Le Règlement Digital Operational Resilience Act (DORA)
- Adoption de 61 amendements par le Sénat
  - Définitions, analyse des dépendances, simplification pour les entreprises, etc.
- Points de vigilance identifiés :
  - Catégorisation de certaines collectivités
  - Création d'une << labellisation NIS 2 >>
  - Différé des dispositions relatives aux contrôles et sanctions
  - Reconnaissance mutuelle entre Etats membre

https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000050349138/

Droit / Juridique / Politique
National

Rejet de l’article 8ter par l’Assemblée nationale

- Loi narcotrafic visant à lutter contre la criminalité
- Intégration de backdoor dans les messageries sécurisées ?
  - Objectif : fournir un accès aux forces de l'ordre pour que les messages échangés puissent être lus
- GROS enjeux de sécurité et de respect des libertés
  - Comment s’assurer que la backdoor ne sera pas abusée par un pirate informatique ?
  - Fin du chiffrement ?
- La CNIL, la Quadrature du Net, les services de messagerie… s’y opposent !
  - Signal menace même de quitter la France
- Résultat : article (amendment) rejeté !

https://www.it-connect.fr/france-lassemblee-nationale-rejette-la-mise-en-place-de-portes-derobees-sur-whatsapp-telegram-etc/

https://www.clubic.com/actualite-555135-avec-la-loi-narcotrafic-signal-quittera-la-france.html

Droit / Juridique / Politique
National

Retour sur les leaks de Free

- Procédure de sanction en cours de discussion par la CNIL
  - Rappel : presque 20 millions d'utilisateurs impactés
  - Accusé d'un manquement à leurs obligations en matière de protection des données personnelles
  - Information de la base de données mise en vente par un mineur

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/la-cnil-ouvre-une-procedure-de-sanction-contre-free-apres-les-fuites-de-donnees-qui-ont-touche-l-operateur-en-2024_7127712.html

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/piratage-massif-de-free-un-jeune-de-17-ans-interpelle-et-presente-a-un-juge-en-vue-de-sa-mise-en-examen_7016000.html

Opérations internationales

Opérations internationales
Opération

Système de fraude aux prothèses auditives stoppé par Europol

- Fraude massive de 6.7 millions € aux subventions de soins de santé
  - Visant le système d'assurance maladie public français
  - Facturation de prothèses auditives qui n’ont jamais été prescrites / livrés ou même existées
  - L’argent récolté a été ensuite blanchi via des dizaines de société écrans en Europe
- Pas besoin d’outil, juste de faux diplômes et de données de patients volées
- Résultats de l’opération :
  - 8 suspects arrêtés
  - 195.000 € saisis, dont 111.000 € sur des comptes bancaires
  - Confiscation d'articles de luxe et d'appareils électroniques
  - Etc.
- Protégez vos données de santé ! #HDS

https://securityonline.info/europol-cracks-down-on-e6-7m-hearing-aid-fraud-scheme-exploiting-french-healthcare/

Opérations internationales
Opération

Saisie de 127 serveurs par la police néerlandaise

- Plateforme d'hébergement << bulletproof >> utilisée par des cybercriminels (dont LockBit)
  - Complice d'avoir soutenu le blanchiment d'argent
  - Utilisation de botnet pour diffusion de malware
- 2 ressortissants russes propriétaires de la plateforme
- Serveurs en cours d'analyse pour recherche d'information sur les ransomwares LockBit et Conti
- Pas d'arrestation des acteurs malheureusement

https://www.it-connect.fr/hebergement-clandestin-127-serveurs-de-zservers-saisis-par-la-police-neerlandaise/

Conférences

Conférences

Passée(s)

- JSSI, 11 mars 2025 à Paris
- CoRIIN, 1er avril 2025 à Lille
- FIC, 1er au 3 avril 2025 à Lille
- sambaXP, 7 au 8 avril 2025 à Göttingen

À venir

- Cyber On Board, 13 au 15 mail 2025 sur la presqu'île de Giens
- BotConf, 20 au 23 mai 2025 à Angers #BoufConf / #BouffeConf
- SSTIC, 04 au 06 juin 2025 à Rennes
- Pass The Salt, 01 au 03 juillet 2025 à Lille
- LeHack « The singularity », 27 au 29 juin 2025 à Paris

Divers / Trolls velus

Divers / Trolls velus
Point

DOGE, modifiable par tous

- Une base de données accessible et modifiable permettant de publier du contenu non autorisé, le tout en libre accès sur le site
  - 2 entrées créés dans la base de données : `<< this is a joke of a .gov site >>` et `<< THESE 'EXPERTS' LEFT THEIR DATABASE OPEN -roro >>`
  - Mauvaise image pour Elon Musk

https://www.lesnumeriques.com/societe-numerique/echec-pour-elon-musk-le-site-de-doge-est-modifiable-par-tout-le-monde-n233136.html

Divers / Trolls velus
Point

PirateFI : un jeu Steam acheté, un malware offert

- 1.500 joueurs piégés
  - Public du 6 au 12 février
  - A l’apparence normale; jeu de survie en monde ouvert, avec des fonctionnalités de construction, de fabrication d’armes et de gestion de ressources + avis positifs sur la plateforme
  - Contient l’infostealer Vidar notamment (c’est cadeau)

https://www.it-connect.fr/un-jeu-steam-nomme-piratefi-infecte-windows-avec-un-malware-voleur-de-donnees/

Divers / Trolls velus
Point

<< Does Firefox sell your personal data? >>

- Réponse :
  - `<< Nope. Never have, never will. And we protect you from many of the advertisers who do. Firefox products are designed to protect your privacy. That’s a promise. >>`
- C’est ce qui **était** inscrit dans le code de Bedrock (mozilla.org)
- Regardons les conditions d’utilisation :
  - `<< When you upload or input information through Firefox, you hereby grant us a nonexclusive, royalty-free, worldwide license to use that information >>`

https://www.mozilla.org/en-US/about/legal/terms/firefox/ (conditions d’utilisation)

https://github.com/mozilla/bedrock/commit/d459addab846d8144b61939b7f4310eb80c5470e

```
59  59              },
60      -           {
61      -               "@type": "Question",
62      -               "name": "Does Firefox sell your personal data?",
63      -               "acceptedAnswer": {
64      -                   "@type": "Answer",
65      -                   "text": "Nope. Never have, never will. And we protect
        you from many of the advertisers who do. Firefox products are designed to
        protect your privacy. That’s a promise. "
66      -               }
67      -           },
68  60              {
```

Divers / Trolls velus
Point

Limitation du nombre de messages externes émis par 24h depuis les tenants O365

- Limite fixée à 10k messages émis / 24h / tenant
- Besoin supérieur : utilisez Azure Communication Services
  - Même pool d'adresses IP mutualisées que les tenants O365 (#SPF)
  - DKIM spécifiques
- Application sur plusieurs temps :

TERRL rollout schedule

Phase	Enable enforcement for tenant group	Rollout start date
1	Tenants with <= 25 email licenses	March 3, 2025
2	+ additional tenants with <= 200 licenses	March 10, 2025
3	+ additional tenants with <= 500 licenses	March 17, 2025
4	+ all remaining tenants	March 31, 2025

https://www.linkedin.com/posts/christophe-dary-85330561_microsoft-azure-communication-activity-7300256648504242176-C_kr/?rcm=ACoAABfYHo0BiCBb5qdB1zQWL8DZKwBfAXdSaDQ

FIN

Prochaine réunion ?

- RDV le **mardi 13 mai 2025**

Accéder aux différents supports ?

Replays

Slides

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

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