Revue d'actualité de l'OSSIR

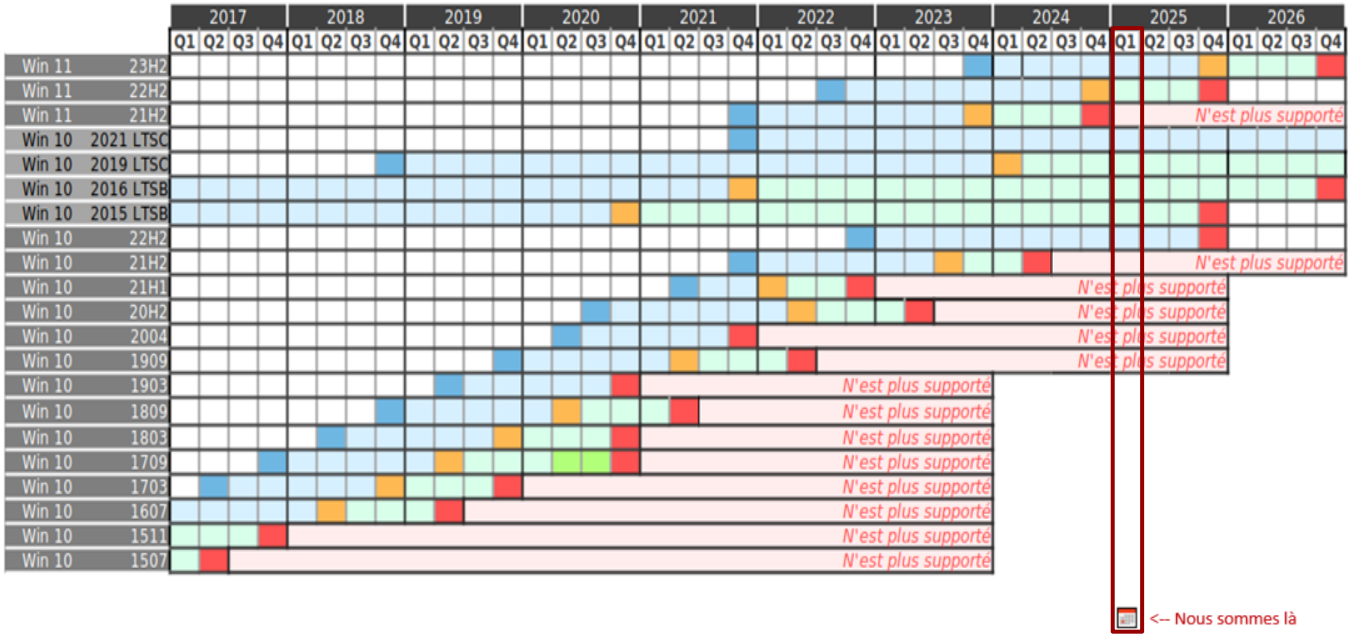
11 février 2025

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

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

Rappel du support Windows en couleurs

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



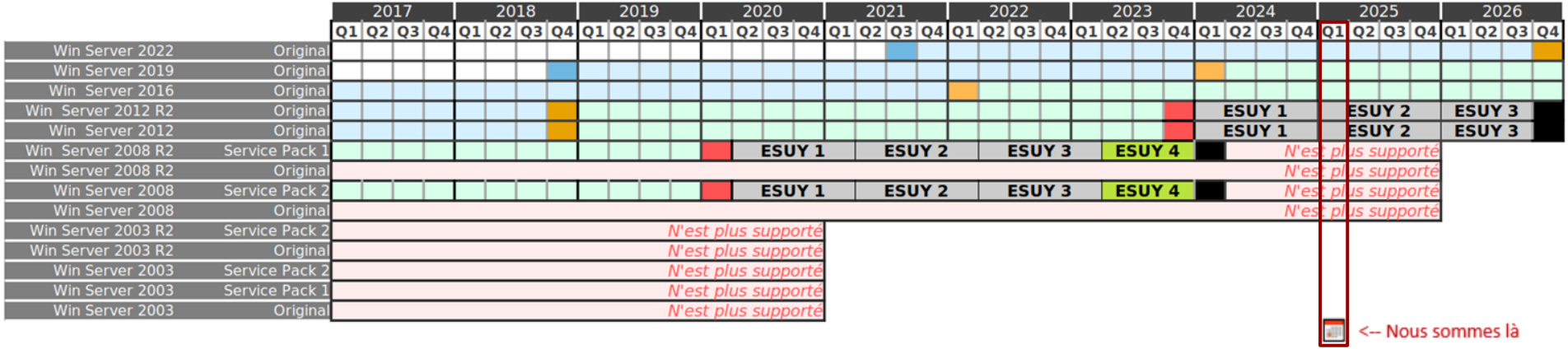
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 18 octobre 2022	mardi 14 octobre 2025	mardi 14 octobre 2025
mardi 16 novembre 2021	jeudi 13 juillet 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 11 mai 2021
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
mercredi 5 avril 2017	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	mardi 9 mai 2017	mardi 9 mai 2017

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour les versions Home, Pro, Pro Education et Pro for Workstations / fin de support standard pour LTSB/LTSC
- Support uniquement pour les versions Enterprise et Education
- Prolongation exceptionnelle suite au Coronavirus
- Fin de support pour toutes les versions / fin de support étendu pour LTSB/LTSC

LTSB : **L**ong-**T**erm **S**ervicing **B**ranch
LTSC : **L**ong-**T**erm **S**ervicing **C**hannel

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



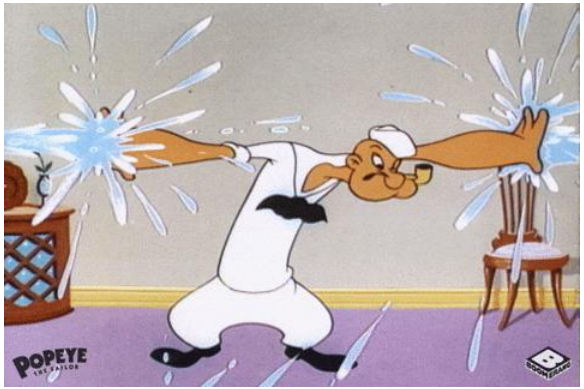
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 30 octobre 2012	mardi 9 octobre 2018	mardi 10 octobre 2023	mardi 13 octobre 2026
mardi 22 février 2011	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
jeudi 22 octobre 2009	mardi 9 avril 2013		
mercredi 29 avril 2009	mardi 13 janvier 2015	mardi 14 janvier 2020	mardi 9 janvier 2024
mardi 6 mai 2008	mardi 12 juillet 2011		
mardi 13 mars 2007	mardi 14 juillet 2015		
dimanche 5 mars 2006	mardi 14 avril 2009		
mardi 13 mars 2007	mardi 14 juillet 2015		
mercredi 30 mars 2005	mardi 14 avril 2009		
mercredi 28 mai 2003	mardi 10 avril 2007		

Légende :

- Date de mise à disposition pour le public et les entreprises
- Support
- Fin de support pour la version standard
- Support étendu pour LTSB/LTSC
- Fin de support étendu pour LTSB/LTSC
- X Extension d'une ou plusieurs années (ESUY)
- X Extension disponible uniquement avec Azure (Microsoft Entra ID)
- Fin de support pour la ou les extensions supplémentaires

ESYC : **E**xtended **S**ecurity **U**pdate **Y**ear

Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de janvier, 159 vulnérabilités patchées dont

- 8 vulnérabilités de type 0-day :
  - [**CVE-2025-21333-21335**] Hyper-V, élévation de privilèges (SYSTEM)
    - Affecte Windows 10 (≥ 22H2) & 11 + Windows Server 2022 & 2025
  - [**CVE-2025-21275**] Installateur de paquets Windows App, élévation de privilèges (SYSTEM)
    - Affecte Windows 10 (≥ 21H2) & 11 + Windows Server 2022 & 2025
  - [**CVE-2025-21308**] Windows Themes, NTLM spoofing
    - Désactiver NTLM (si possible) et filtrer le trafic NTLM (qui ne doit pas sortir de votre organisation)
  - [**CVE-2025-21186|21366|21395**] Microsoft Access, RCE
    - .accdb, .accde, .accdw, .accdt, .accda, .accdr et .accdu bloqués s'ils sont envoyés par mail
    - Affecte Access 2016, Office 2019, Office LTSC 2021 et 2024 ainsi que Microsoft 365 Apps for Enterprise
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2025-21380**] Azure Marketplace SaaS Resources, fuite d'informations
  - [**CVE-2025-21296**] BranchCache, RCE
  - [**CVE-2025-21294**] Microsoft Digest Authentication, RCE
  - [**CVE-2025-21362|21354**] Microsoft Office - Excel, RCE
  - [**CVE-2025-21385**] Microsoft Purview, fuite d'informations
  - [**CVE-2025-21307**] RMCAST - Reliable Multicast Transport Driver, RCE
  - [**CVE-2025-21311**] Windows - NTLM, élévation de privilèges
  - [**CVE-2025-21298**] Windows - OLE, RCE **(on en parlera plus tard)**
  - [**CVE-2025-21309|21297**] Windows - Services Bureau à distance (RDS), RCE
  - [**CVE-2025-21295**] Windows - SPNEGO Extended Negotiation, RCE

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

Failles / Bulletins / Advisories
Systèmes

6 vulnérabilités dans Rsync (l'outil)

- `<< Les attaquants peuvent prendre le contrôle d'un serveur malveillant et lire/écrire des fichiers arbitraires de n'importe quel client connecté >>` #CERT/CC
  - [**CVE-2024-12084**] << Buffer-overflow >> dans les sommes de contrôle
  - [**CVE-2024-12085**] Fuite d'informations via un contenu de pile (stack) non initialisé
  - [**CVE-2024-12086**] Fuite de fichiers arbitraires via un serveur Rsync
  - [**CVE-2024-12087**] << Path traversal >> dans Rsync
  - [**CVE-2024-12088**] Bypass de l'option --safe-links entraînant un << Path traversal >>
  - [**CVE-2024-12747**] << Race condition >> dans la gestion des liens symboliques
  - Scénario de compromission : récupération des clés SSH présentes sur le serveur
- Toutes les versions ≤ 3.4.0 (dernière sortie le 14/01/2025)
- Quelques actions de mitigation si besoin :
  - Désactiver le support SHA* en compilant Rsync avec des options spécifiques
    - `CFLAGS=-DDISABLE_SHA512_DIGEST` et `CFLAGS=-DDISABLE_SHA256_DIGEST`
  - Utiliser l'option de compilation `-ftrivial-auto-var-init=zero` pour initialiser vous-même la pile (à 0)

https://www.it-connect.fr/linux-mettez-a-jour-rsync-pour-vous-proteger-de-6-vulnerabilites-importantes/

Failles / Bulletins / Advisories
Systèmes

La vulnérabilité critique Windows du moment


CVE-2025-21298

- 0-click dans Windows OLE permettant une RCE
  - RCE par mail !
  - Obtention des mêmes privilèges que le compte utilisateur actuel
- Déclenchement lors de l'ouverture ou de la prévisualisation d'un mail 💀 dans Outlook
  - Mail contenant un fichier RTF malveillant
- Merci la bibliothèque *ole32.dll* (fonction oletOlePresStmToContentsStm)

https://www.offsec.com/blog/cve-2025-21298/

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

Active Directory, élévation de privilège

CVE-2025-21293

- Faiblesse située au niveau du groupe de sécurité nommé << Opérateurs de configuration réseau >> (Network Configuration Operators), disponible par défaut dans un AD
  - Anomalie dans les droits de la liste de contrôle d'accès des groupes d'utilisateurs, liée à l'attribut << CreateSubKey >> sur deux clés du registre liées à des services : DnsCache et NetBT
  - Exploitation passant par l'Analyseur de Performances de Windows (PerfMon.exe) ou de WMI
    - Créer des valeurs dans le Registre (sous DnsCache, par exemple)
    - Enregistrement d'une DLL malveillante qui sera ensuite lue par l'Analyseur de Performances, menant à une élévation de privilèges associée à une exécution de code en tant que SYSTEM

https://www.it-connect.fr/active-directory-code-exploitation-faille-de-securite-cve-2025-21293/

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

Clone2Leak : failles dans les outils Git

- Présentes dans GitHub Desktop, Git LFS, GitHub CLI/Codespaces & GitHub Credential Manager
  - Possible de compromettre les mots de passe et jetons d'accès
  - Faiblesses dans les helpers d'authentification lors de la connexion avec des dépôts distants
  - Problème avec le retour chariot de l'application Desktop et CM
  - Ajout de nouvelles lignes dans les fichiers `<< .lfsconfig >>` de manière inapproprié sur GIT LFS
- Versions patchées →
  - GitHub Desktop 3.4.12
  - Git Credential Manager 2.6.1
  - Git LFS 3.6.1
  - gh cli 2.63.0

https://www.it-connect.fr/clone2leak-comment-des-failles-git-font-fuiter-vos-identifiants/

CVE-2025-23040
CVE-2025-50338
CVE-2025-53263
CVE-2025-53858

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

Bitwarden : 3 CVE importantes

CVE-???
CVE-2025-24364
CVE-2025-24365

- Accès au panneau d'administration via CSRF
  - Si l'option : DISABLE_ADMIN_TOKEN est activée, permet d'inciter un utilisateur authentifié à visiter une page Web malveillante pour envoyer des commandes au panneau d'administration
- Exécution de code à distance dans le panneau d'administration
  - Permet à un attaquant authentifié d'exécuter du code sur le serveur
- Escalade de privilège via une << Variable Confusion >>
  - Présente dans OrgHeaders permettant aux attaquants d'obtenir les droits de propriétaire d'autres organisations et potentiellement accéder à des données sensibles
- Version patchée → 1.33.0

https://securityonline.info/password-management-at-risk-vaultwarden-vulnerabilities-expose-millions/

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

Veeam Updater, 1 CVE avec de nombreux impacts

CVE-2024-23114

- Permet de réaliser une attaque de type MitM
  - Exécution de code sur le serveur avec des accès root
- Impacts sur les produits et versions suivantes :
  - Veeam Backup *pour Salesforce* — 3.1 et plus
  - Veeam Backup *pour Nutanix AHV* — 5.0 | 5.1
  - Veeam Backup *pour AWS* — 6a | 7
  - Veeam Backup *pour Microsoft Azure* — 5a | 6
  - Veeam Backup *pour Google Cloud* — 4 | 5
  - Veeam Backup *pour Oracle Linux Virtualization Manager et Red Hat Virtualization* — 3 | 4.0 | 4.1

https://socradar.io/veeam-cve-2025-23114-servers-remote-code-execution/

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

2 vulnérabilités dans le framework Linux kernel’s eBPF

- Permet aux programmes de s'exécuter dans l'espace du noyau Linux sans nécessiter de modules du noyau ou de recompilation
  - Choix populaire pour le réseau, la sécurité et le traçage
- << Buffer overflow >> sur des fonctions critiques
  - xsk_map_delete_elem et devmap_map_delete_elem

https://securityonline.info/cve-2024-56614-cve-2024-56615-poc-exploits-released-for-severe-ebpf-vulnerabilities-in-linux-kernel/

CVE-2024-56614
CVE-2024-56615

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

Faille côté LLM de Meta (Llama)


CVE-2024-50050

- Exécution de code possible sur le serveur lama-stack
  - Possible via une désérialisation non contrôlée
  - CVSS de 6.3, mais Snyk l'évalue à 9.3
- Lama Stack ?
  - Ensemble d'interfaces API pour le développement et l'utilisation, entre autres, de Llama
  - Une désérialisation automatique des objets Python utilisant pickle
    - Format jugé à risque car vulnérables à plusieurs RCE
- Passez à une version lama-stack ≥ 0.0.41

https://security.snyk.io/vuln/SNYK-PYTHON-LLAMASTACK-8302915 (rapport de Snyk)

https://thehackernews.com/2025/01/metas-llama-framework-flaw-exposes-ai.html?m=1

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

Nouvelle faille critique côté WordPress

CVE-2024-12365

- Affecte le plugin W3 Total Cache
  - Dans toutes ses versions !
- Se situe dans la fonction << is_w3tc_admin_page >>
  - Absence de vérification des permissions
    - Un simple utilisateur (authentifié donc) peut mener des attaques SSRF 😲
  - Risques :
    - Divulgation d'informations critiques, saturation des services de cache, ralentissement des performances, etc.
- Comment s'en protéger alors ???
  - Correctif disponible pour la version 2.8.2 du plugin
  - Des centaines de milliers de sites toujours vulnérables…

https://www.clubic.com/actualite-550556-encore-une-faille-dans-un-plugin-wordpress-1-million-de-sites-exposes-a-des-fuites-de-donnees.html

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

Faille importante chez AnyDesk

CVE-2024-12754

- Permet d’obtenir un accès non autorisé aux fichiers système sensibles
- Via le traitement de l’image d’arrière plan du bureau lors de l’ouverture de la session
  - Copie du fond d’écran dans /Temp avec le compte NT AUTHORITY\SYSTEM
  - Possible de rediriger cette copie vers des fichiers sensibles (SAM) avec des liens symboliques
- POC démontrant la vulnérabilité
  - Permet de manipuler les opérations de fichiers dans les répertoires Windows Object Manager Namespace (OMNS) tels que \RPC Control.

https://github.com/CICADA8-Research/Penetration/tree/main/POCs/CVE-2024-12754?s=09

https://cybersecuritynews.com/poc-exploit-released-for-anydesk-vulnerability-exploited/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Départ compliqué pour le ChatGPT chinois du moment

- 20 janvier 2025 : DeepSeek fourni son LLM Open Source DeepSeek R1 sur GitHub
  - https://github.com/deepseek-ai/DeepSeek-R1
  - Gros succès !
- 27 janvier 2025 : jailbreak trouvé permettant de créer du contenu malveillant via le LLM
  - Selon KELA, le modèle R1 serait beaucoup plus vulnérable que ChatGPT sur cette partie
    - Rapport de KELA : 28 janvier 2025 : attaques DDoS sur ses serveurs
  - Inscriptions perturbées quelques heures
- 28 janvier 2025 : attaques DDoS sur ses serveurs
  - Inscriptions perturbées quelques heures
- 30 janvier 2025 : première fuite de données
  - Base de données ClickHouse accessible publiquement sans authentification requise
    - oauth2callback.deepseek.com:9000 et dev.deepseek.com:9000 + requêtes SQL = 💥
  - Historique des conversations (en clair), clés API, détails sur l'infrastructure, logs, etc.

https://www.kelacyber.com/blog/deepseek-r1-security-flaws/ (rapport de KELA)

https://www.bleepingcomputer.com/news/security/deepseek-halts-new-signups-amid-large-scale-cyberattack/

https://securityonline.info/deepseeks-exposed-database-leaks-sensitive-user-information/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

RID hijacking

- Technique assez connue (apparue en 2018) mais toujours aussi efficace !
- Utilisée par le groupe Lazarus pour créer un compte administrateur sous Windows
  - Transforme un compte à faible privilège en admin
  - Se base sur une identification du RID (Relative Identifier)
- Nécessite des outils disposant de droits SYSTEM comme PsExec
  - Création d'un compte masqué à faible privilège
  - Modification du RID
  - Effacement des traces
- Comptes disposent des droits admin et accès à distance, assurant la persistance
- Recommandation :
  - Désactiver la création de comptes invités et l'utilisation d'outil tels que PsExec ou JuiciPotato

https://www.it-connect.fr/windows-rid-hijacking-utilisee-par-pirates-pour-creer-un-compte-admin-cache/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Exploitation d’une faille 0-day sur 7-Zip contre l’Ukraine

- CVE-2025-0411, patchée en novembre 2024 (v24.09)
  - Permet aux attaquants de contourner la protection Mark of the Web (MotW)
    - Applique un tag sur les fichiers indiquant qu’ils proviennent d’Internet et leur permet d'être analysés par Windows Defender
- Utilisation d’homoglyphes pour usurper l'identité de sites web légitimes afin d'inciter les utilisateurs à saisir leurs informations d'identification en vue d'une collecte d'informations
- Objectif :
  - Faire passer des fichiers exécutables pour des documents

https://www.it-connect.fr/cyberguerre-des-pirates-russes-ont-exploite-une-faille-de-7-zip-contre-lukraine/

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Attaque par force brute à grande échelle (en cours)

- Depuis le mois dernier, ciblant les appareils exposés notamment Palo Alto Networks, Ivanti et SonicWall
  - Etude réalisée par The Shadowserver Foundation
  - Pret de 2.8 millions d'IP sources

https://www.bleepingcomputer.com/news/security/massive-brute-force-attack-uses-28-million-ips-to-target-vpn-devices/

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

15.000 fichiers de configuration de FortiGate dans la nature

- Configuration complète + identifiants de connexion
  - Noms d'utilisateur, mots de passe (certains en clair !), certificats, règles de pare-feu…
- Liste des pare-feu organisée par pays (c'est gentil)
- Aucun lien avec la CVE-2024-55591
  - Données datant d'octobre 2022
  - CVE-2022-40684 plutôt ?
- (une) Résolution 2025 proposée :
  - Ne pas exposer l'interface admin de ses équipements sur Internet 😁

https://www.it-connect.fr/15-000-firewalls-fortigate-menaces-fuite-massive-config-complete-et-identifiants/

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

Des millions de données de voyageurs exposées

- 25 millions d'enregistrements de données
  - Relatifs à des clients du groupe Honotel (acteur français et européen dans l'hôtellerie)
  - Noms, prénoms, adresses mail, n° de téléphone, dates de naissance, détails des séjours, etc.
- Combo de serveurs exposés << Elastisearch & Kibana >>
  - Découverte réalisée par Cybernews
    - Sécurisation effectuée immédiatement après (mais déjà trop tard…)

https://www.01net.com/actualites/fuite-massive-groupe-francais-expose-donnees-millions-voyageurs.html

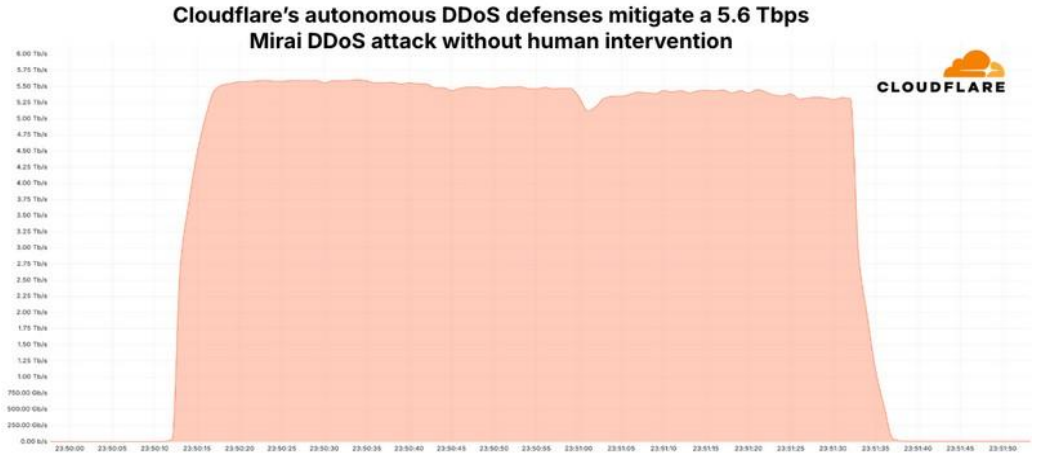
Piratages, Malwares, spam, fraudes et DDoS
Pannes

Mirai vs CloudFlare : attaque DDoS record bloquée 🥇

- 5,6 térabits par seconde (Tbps) !
- Attaque orchestrée par Mirai : 13.000 machines zombies
  - Protocole UDP utilisé
  - Cible : fournisseur d'accès à Internet (FAI) en Asie de l'Est
- A eu lieu le 29 octobre 2024, pendant 80 secondes

https://blog.cloudflare.com/fr-fr/ddos-threat-report-for-2024-q4/ (article de CloudFlare sur le sujet)

https://www.it-connect.fr/botnet-mirai-cloudflare-a-bloque-une-attaque-ddos-record-de-56-tbps/



Piratages, Malwares, spam, fraudes et DDoS
Pannes

ChatGPT : Le robot d'indexation fait du DDoS

- Lié à la possibilité de pouvoir faire des recherches sur internet depuis le ChatGPT-User
  - Utilisation du crawler pour réaliser un DDoS sur un site web
  - Possible de faire entre 5 et 20.000 requêtes par seconde
  - Attaque réalisable sans authentification sur ChatGPT
- Faille signalée à OpenAI et Microsoft
  - Aucune réponse, ni changement → vulnérabilité toujours présente

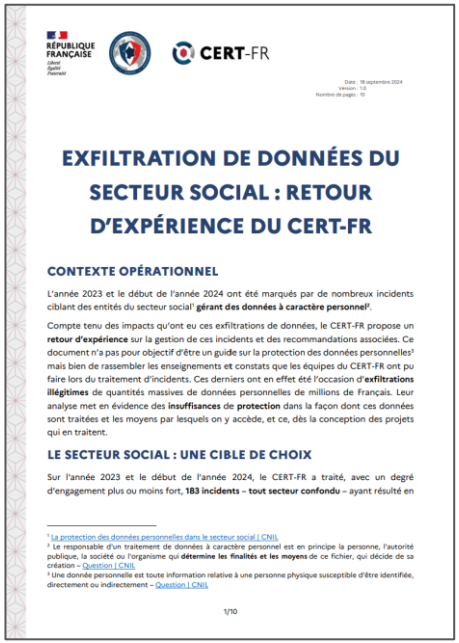
https://www.it-connect.fr/faille-robot-indexation-chatgpt-utilise-pour-lancer-des-attaques-ddos/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Rapport du CERT-FR

- RETEX sur l'exfiltration de données du secteur social 2023/2024
- Constats effectués :
  - Sensibilité des données sous-estimée
  - Accès non sécurisés
  - Vulnérabilités techniques
- Recommandations de l'ANSSI :
  - Renforcer la sécurité des applications
  - Sensibiliser les acteurs
  - Adopter une approche de sécurité dès la conception

https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-009/ (rapport)



RÉPUBLIQUE FRANÇAISE

CERT-FR

EXFILTRATION DE DONNÉES DU SECTEUR SOCIAL : RETOUR D'EXPÉRIENCE DU CERT-FR

CONTEXTE OPÉRATIONNEL

L'année 2023 et le début de l'année 2024 ont été marqués par de nombreux incidents ciblant des entités du secteur social[1] **gérant des données à caractère personnel**[2].

Compte tenu des impacts qu'ont eu ces exfiltrations de données, le CERT-FR propose un **retour d'expérience** sur la gestion de ces incidents et des recommandations associées. Ce document n'a pas pour objectif d'être un guide sur la protection des données personnelles[3] mais bien de rassembler les enseignements et constats que les équipes du CERT-FR ont pu faire lors du traitement d'incidents. Ces derniers ont en effet été l'occasion d'**exfiltrations illégitimes** de quantités massives de données personnelles de millions de Français. Leur analyse met en évidence des **insuffisances** de **protection** dans la façon dont ces données sont traitées et les moyens par lesquels on y accède, et ce, dès la conception des projets qui en traitent.

LE SECTEUR SOCIAL : UNE CIBLE DE CHOIX

Sur l'année 2023 et le début de l'année 2024, le CERT-FR a traité, avec un degré d'engagement plus ou moins fort, **183 incidents** – **tout secteur confondu** – ayant résulté en

[1] La protection des données personnelles dans le secteur social | CNIL
[2] Le responsable d'un traitement de données à caractère personnel est en principe la personne, l'autorité publique, la société ou l'organisme qui **détermine les finalités et les moyens** de ce fichier, qui décide de sa création – Question | CNIL
[3] Une donnée personnelle est toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement – Question | CNIL

1/10

Piratages, Malwares, spam, fraudes et DDoS
Publication

Rapport de Google concernant le Google Play Store

- Quelques chiffres :
  - 2.36 millions d'applications interdites d'entrer dans le Store
  - 1.3 million d'applications empêchées d'avoir un accès excessif aux données sensibles des utilisateurs
  - 158.000 comptes développeurs bannis
- Google est fière de son outil Google Play Protect qui a analysé plus de 200 milliards d'appli.
- Nouvelles fonctionnalités sur les Android :
  - Révocation automatique des applications potentiellement dangereuses
  - Chrome rappelle de réactiver Google Play Protect si la fonctionnalité a été désactivée
  - Impossible de désactiver Google Play Protect lors des appels téléphoniques ou vidéo
- Autres informations liées à l'API Play Integrity, l'utilisation de l'IA, des chiffres…

https://security.googleblog.com/2025/01/how-we-kept-google-play-android-app-ecosystem-safe-2024.html (rapport)

Blue Team Gestion des Dev Tunnels via des stratégies de groupe

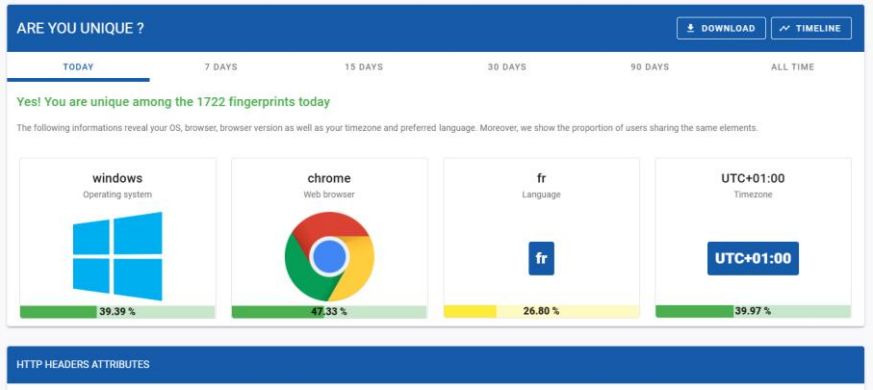
- Accessibles via Visual Studio, Visual Studio Code ou encore via la CLI (devtunnel)
- Prise en charge maintenant via des stratégies de groupe
  - Modèles au formats ADMX/ADML
- Prérequis :
  - OS : Windows Server 2016, 2019, 2022, Windows 8.1, 10, 11
  - Accès à l'éditeur de stratégies de groupe
    - Outil GPO (cas AD) ou stratégies de groupe local (cas workstation)
- Stratégies de groupe disponibles :
  - << Désactiver l'accès anonyme aux tunnels >>
  - << Désactiver les Dev Tunnels >>
  - << Autoriser uniquement des ID de locataire Microsoft Entra sélectionnés >>

https://techcommunity.microsoft.com/blog/azuredevcommunityblog/manage-dev-tunnels-with-group-policies/4149472

Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

My Browser Fingerprint

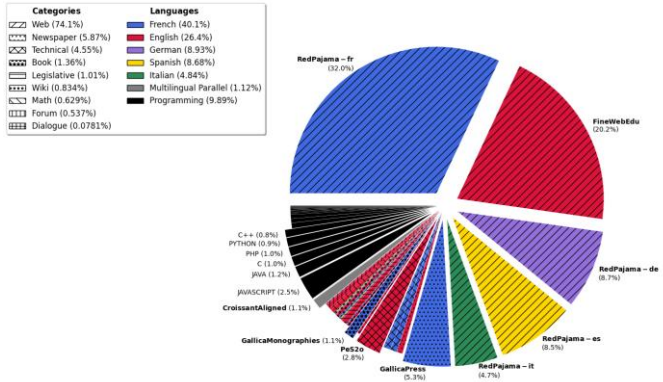
- Vers une fin des cookies remplacés par fingerprinting plus avancé
  - Impossible à bloquer ou à effacer (contrairement aux cookies)
    - L'ICO n'est pas d'accord avec cette pratique et ça se comprend !
- Des solutions existent pour limiter le fingerprinting
  - Navigateurs : Firefox (Enhanced Tracking Protection), Brave
  - Extensions web : Canvas Defender, Privacy Badger
  - Désactiver le JS par défaut sur les sites que vous visitez ainsi que Flash (👀)
- Evaluer votre navigateur avec : https://amiunique.org/fingerprint



Piratages, Malwares, spam, fraudes et DDoS
Techniques & outils

Dataset d'entraînement de Lucie (LLM) disponible gratuitement

- Disponible où ? https://huggingface.co/datasets/OpenLLM-France/Lucie-Training-Dataset
- Dataset utilisé pour le modèle de Lucie à 7 milliards de paramètres (7B)
- Quelles données présentes dans ce modèle ?
  - \+ de données en français qu'en anglais (pour minimiser les biais culturels anglo-centriques)
  - Données présentes également dans d'autres langues en petite quantité : allemand, espagnol et italien
  - Sources : web, journaux, forums, textes législatifs, wiki, codes, etc.
- Sources des données présentes dans le Git
  - Ainsi que le format des données, le filtrage qui a été effectué, etc.
- Entrainez vos IA !
  - Dataset publié sous CC BY-NC-SA 4.0



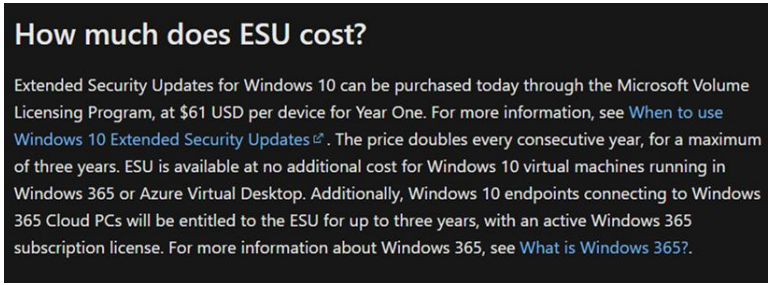
Business et Politique

Business
Monde

Mises à jour étendues pour Windows 10 à partir de 61$ / ordinateur (entreprise)

- 61$ la première année, puis x2 l'année d'après, puis x2 encore
  - Support étendu pendant 3 ans max.
- ESU cumulatives !
  - = si vous décidez d'acheter le programme la 2ème année, il faudra également payer pour la 1ère
- Mises à jour gratuites dans certains cas :
  - Utilisation d'un PC sous Windows 10 pour se connecter sur un PC cloud Microsoft 365
  - Utilisation de VM (machine virtuelle) Windows 10 exécutant Microsoft 365 ou Azure Virtual Desktop
- Encore 60.37% des Windows Workstation dans le monde sont des Windows 10…

https://windows.developpez.com/actu/368842/Les-mises-a-jour-de-securite-etendues-de-Microsoft-pour-Windows-10-commencent-a-61-par-ordinateur-pour-les-entreprises-et-ce-prix-doublera-chaque-annee-pendant-une-periode-de-trois-ans/



How much does ESU cost?

Extended Security Updates for Windows 10 can be purchased today through the Microsoft Volume Licensing Program, at $61 USD per device for Year One. For more information, see When to use Windows 10 Extended Security Updates. The price doubles every consecutive year, for a maximum of three years. ESU is available at no additional cost for Windows 10 virtual machines running in Windows 365 or Azure Virtual Desktop. Additionally, Windows 10 endpoints connecting to Windows 365 Cloud PCs will be entitled to the ESU for up to three years, with an active Windows 365 subscription license. For more information about Windows 365, see What is Windows 365?.

Droit / Juridique / Politique
Monde

Compte rendu de la CNIL sur son année 2024

- 87 sanctions pour un montant total de 55.212.400 €
  - 21 en 2022 et 42 en 2023
- 12 décisions rendues publiques, exemples marquants :
  - Scraping sauvage de LinkedIn par Kaspr (240.000 €)
  - Insertion de publicité par Orange entre les mails de ses utilisateurs sans leur accord (50 millions €)
- 180 mises en demeures
  - Concerne, en partie, plusieurs établissement de santé
  - Ciblent également plusieurs bannières de cookies trompeuses
- Autres chiffres :
  - 72 amendes dont 14 avec injonctions sous astreinte
  - 8 décisions de liquidation d'astreinte
  - 4 rappels à l'ordre

https://next.ink/169220/la-cnil-se-felicite-des-87-sanctions-quelle-a-prises-en-2024/

Opérations internationales

Opérations internationales

<< Operation Talent >> #Europol

- À l’assaut des forums et marchés de la cybercriminalité
  - Participants : Etats-Unis, Roumanie, Australie, France, Allemagne, Espagne, Italie et Grèce
- Fin de cracked[.]io et de nulled[.]to
  - Serveurs et noms de domaine saisis
- Prochains sur la liste :
  - sellix[.]io
  - mysellix[.]io
  - starkrdp[.]io

https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation

Opérations internationales

Fin de 8base #Europol

- Gang de ransomware arrêté
  - Apparu début mars 2022 et très actif depuis juin 2023
  - 2 hommes et 2 femmes
- Responsable de + de 16M€ avec + 1.000 victimes

https://www.linkedin.com/posts/clementdomingo_cyberalert-une-op%C3%A9ration-polici%C3%A8re-activity-7294758641503490050-fV3L

Conférences

Conférences

À venir

- JSSI, 11 mars 2025 à Paris
  - Sujet : << Le Cloud >>
  - Donc pas de revue d'actualités le mois prochain ℹ️
- CoRIIN, 1er avril 2025 à Lille
  - En parallèle du FIC
- FIC, 1er au 3 avril 2025 à Lille

Divers / Trolls velus

Divers / Trolls velus

Fin des notifications d’expiration de certificat par Let’s Encrypt

- Prévue à partir du 4 juin 2025
- Raisons ?
  - Plus besoin de conserver les @ mails liés aux demandes de certificat #confidentialité
  - Coût de plusieurs milliers de $ pour un tel service en moins #économie
- Mais du coup, on fait comment ?
  - Automatiser le renouvellement
  - Faite vous-même votre SSL monitoring
    - Script bash avec openssl et le tour est joué !

https://letsencrypt.org/2025/01/22/ending-expiration-emails/

Divers / Trolls velus

Fonction cachée activé par défaut sur vos Livebox (merci Orange)

- CGNAT activé ! C’est quoi ?
  - Fonctionnalité qui permet à plusieurs utilisateurs de partager une même adresse IPv4
  - Plusieurs réseaux privés sous une seule adresse publique
- Réponse à une pénurie d’adresses IPv4
  - Oui, mais prévenez avant d’activer ce genre d’option…
- Confusion juridique possible, mise hors service de certaines redirections de port, etc.
- Possibilité de désactiver l’option depuis l’interface web (rubrique << Réseau >>)

https://www.universfreebox.com/article/576218/orange-active-une-nouvelle-fonctionnalite-sur-ses-livebox-qui-nest-pas-sans-defauts

Divers / Trolls velus

La déconnexion de votre compte Microsoft sur navigateur ne sera plus automatique

- Changement dès… février (on y est) !
- L'option << Stay signed in ? >> va disparaitre, Microsoft choisira << oui >> pour vous
- Ce que ça implique ?
  - Risque dans le cas où vous utilisez une machine publique (université, kiosque, etc.)
  - Vol de session, accès non désirés, etc.
- Vous pouvez toujours utilisez la navigation privée !

https://www.it-connect.fr/fevrier-2025-microsoft-vous-maintiendra-automatiquement-connecte-a-votre-compte/

Divers / Trolls velus

3 millions de serveurs de messagerie vulnérables

- Etude réalisée par The Shadow Server à l'échelle mondiale
  - Vulnérables dû à une mauvaise configuration
  - Autorisent le trafic IMAP et POP3 non sécurisé (110/TCP ou 995/TCP sans support TLS)
- Recommandation :
  - Vérifiez les certificats TLS 1.3 (de préférence)
  - Mettre en place des Tags contre le spam et le phishing (DMARC, DKIM, SPF, RBL)

https://www.it-connect.fr/3-millions-de-serveurs-messagerie-exposent-les-e-mails-des-utilisateurs/

Youtube, repaire des influenceurs et des pirates

- Piègent des victimes cherchant des tutoriels d'installation de logiciels
  - Contiennent des liens vers des sites de téléchargements qui dissimulent des malwares.
  - Rappel d'une campagne d'un MaaS sur Youtube avec pour objectif le vol des données sensibles

https://www.it-connect.fr/les-pirates-ciblent-les-utilisateurs-via-youtube-et-google-pour-distribuer-des-malwares-voleurs-de-donnees/

Divers / Trolls velus

Partager son RIB, conséquence ?

- Partage de RIB en masse sur Twitch
  - Chaîne de l'influenceur Nasdas dans le but de faire des dons
  - Usurpation d'identité suite aux messages dans le chat
- CNIL : guide en cas de fuite d'IBAN
- En cours de discussion d'un point de vue juridique par rapport aux principes du RGPD

https://next.ink/169115/echec-collectif-des-rib-partages-en-direct-sur-twitch-a-la-demande-dun-influenceur/

Projet Stargate, initiative IA américaine

- Réunis de grand acteurs financiers comme SoftBank, MGX et techniques comme NVIDIA, Microsoft, OpenIA
  - Construction d'un centre de données au Texas
  - 500 milliards de dollars vont être investis dans ce projet sur 4 ans

https://next.ink/166568/intelligence-artificielle-stargate-le-projet-fou-americain-a-500-milliards-de-dollars/

FIN

Prochaine réunion ?

- RDV le **mardi 08 avril 2025**

Accéder aux différents supports ?

Replays

Slides

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

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