Revue d'actualité de l'OSSIR

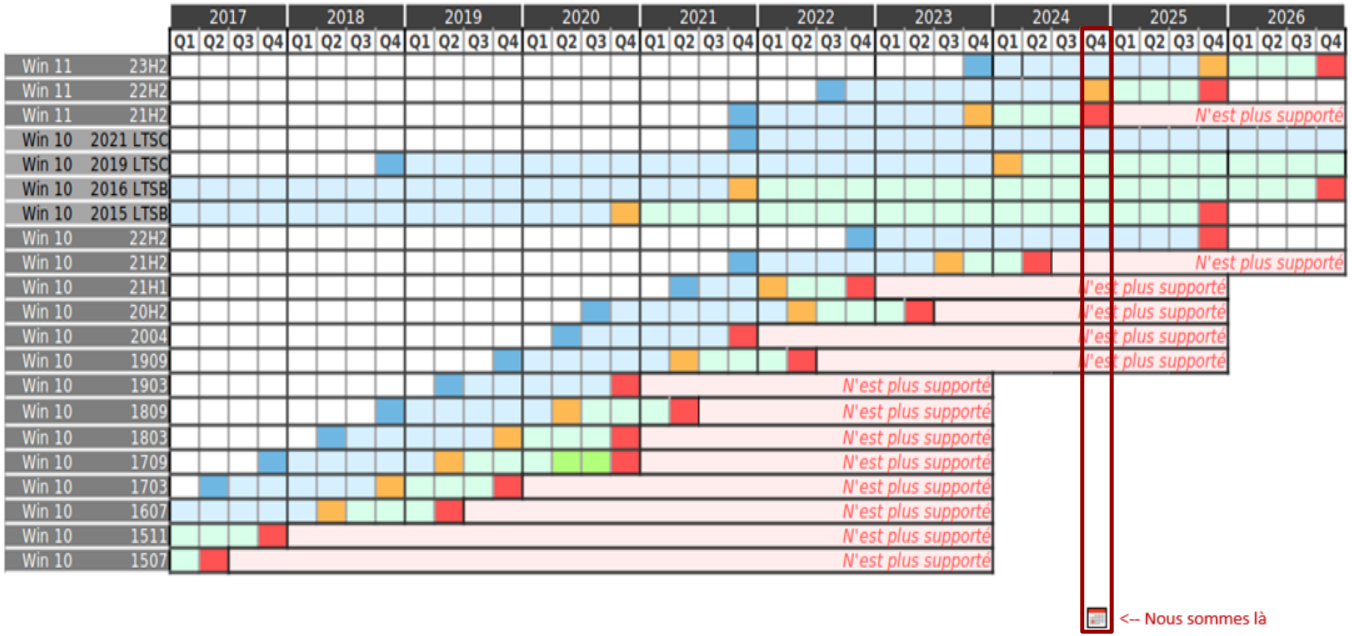
08 octobre 2024

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***



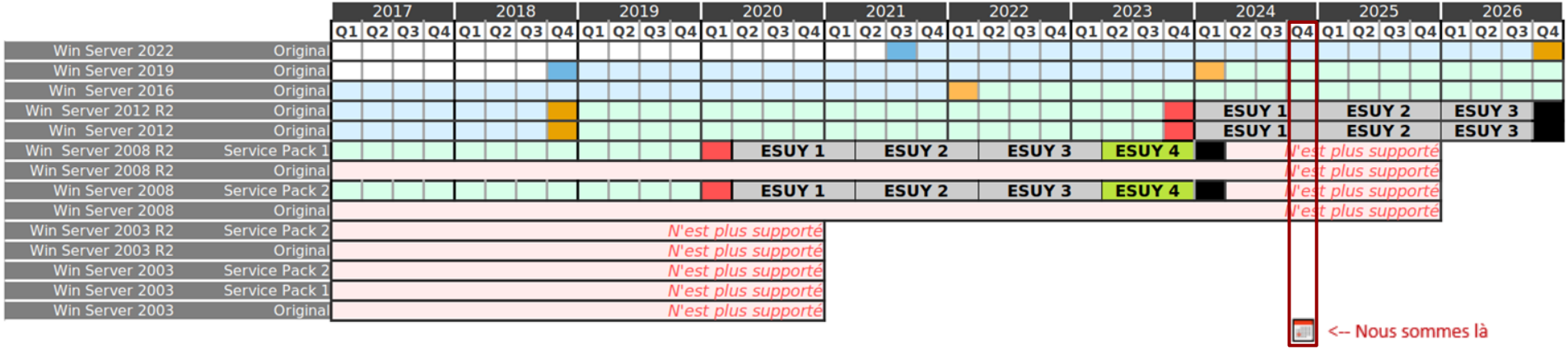
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



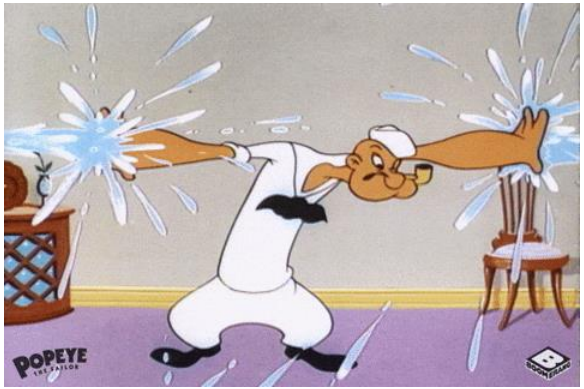
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 septembre, 79 vulnérabilités patchées dont

- 4 vulnérabilités de type 0-day :
  - [**CVE-2024-38014**] Elévation de privilèges, **Windows Installer**
    - Affecte Windows 10 & 11 (workstation) et Windows Server ≥ 2008
  - [**CVE-2024-38217**] Contournement du **Mark of the Web**
    - Exploitée activement depuis 2018 - associée à la technique **LNK stomping**
    - Affecte Windows 10 & 11 (workstation) et Windows Server ≥ 2008
  - [**CVE-2024-38226**] Contournement des sécurités contre les macros, **Microsoft Publisher**
    - Affecte Microsoft Office 2016, Office 2019 et Office 2021 LTSC
  - [**CVE-2024-43491**] Downgrade de l'OS, **Windows Update**
    - Vulnérabilité dans la fonction **Servicing Stack**
    - Affecte Windows 10 version 1507 (plus supportée…) et Windows 10 (IoT) Enterprise 2015 LTSB
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2024-38216** & **CVE-2024-38220**] Elévation de privilèges, **Azure Stack Hub**
  - [**CVE-2024-38194**] Elévation de privilèges, **Azure Web Apps**
  - [**CVE-2024-43464** & **CVE-2024-38018**] RCE, **Microsoft SharePoint**
  - [**CVE-2024-38119**] RCE, **Windows NAT**
  - [**CVE-2024-43491**] RCE, **Windows Update**

https://www.it-connect.fr/patch-tuesday-septembre-2024-failles-de-securite-microsoft/

Failles / Bulletins / Advisories
Systèmes

Bornes Wi-fi Aruba “Arua Access Points”

- 3 vulnérabilités critiques : RCE en UDP sur port 8211
  - Certaines versions ne sont pas corrigés, liste disponible sur le site HPE :
  - Versions vulnérables : ---------->
    - **AOS-10.6.x.x** : 10.6.0.2 et inférieur
    - **AOS-10.4.x.x** : 10.4.1.3 et inférieur
    - **Instant AOS-8.12.x.x** : 8.12.0.1 et inférieur
    - **Instant AOS-8.10.x.x** : 8.10.0.13 et inférieur

https://www.it-connect.fr/hpe-aruba-3-failles-critiques-decouvertes-dans-les-points-dacces-wi-fi/

Failles / Bulletins / Advisories
Systèmes

Failles critiques dans CUPS 🖨️

- CUPS = Common UNIX Printing System
  - Système d'impression le plus répandu sur les systèmes Linux, FreeBSD, OpenBSD et NetBSD
- Failles sur plusieurs librairies :
  - **CVE-2024-47076** → libcupsfilters
  - **CVE-2024-47175** → libppd
  - **CVE-2024-47176** → cups-browsed
  - **CVE-2024-47177** → cups-filters
- Si cups-browsed 👺 activé + en écoute sur le port 631/UDP = 💣💥💥
  - Installation automatique d'une imprimante détectée sur le réseau
  - Quid si l'imprimante est malveillante et contient un PDD ? RCE !
- Désactivez le service (s'il est activé) et filtrer le port 631/UDP
  - `$ systemctl stop cups-browsed && systemctl disable cups-browsed`

https://socradar.io/cups-vulnerabilities-what-you-need-to-know/

Failles / Bulletins / Advisories
Systèmes

Equipements My Cloud vulnérables

- Une dizaine d'équipements My Cloud vulnérables chez Western Digital
- RCE découvert par Claroty Research – Team82 – Noam Moshe en collaboration avec Trend Micro Zero Day Initiative
  - Exploitable dans une attaque MITM
  - Possible d'injecter des payloads lors des demandes de maj DNS auto entraînant un débordement de tampon

https://securityonline.info/cve-2024-22170-cvss-9-2-western-digital-addresses-critical-flaw-in-my-cloud-devices/

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Arc Browser, comment compromettre n'importe quel client à distance ? (CVE-2024-45489)

- Rappel : vous avez besoin d'un compte pour utiliser le navigateur
  - Suivi des mises à jour, questions, commentaires, etc.
- Possibilité d'utiliser des << Arc Boost >>
  - Scripts permettant de personnaliser les sites web voulus (custom CSS et JS)
  - Besoin d'un creator ID pour associer le boost à un compte
- Et si on soumet le boost avec un creator ID qui ne nous appartient pas ?
  - Le boost s'appliquera à un compte qui n'a rien demandé
- Pourquoi les boosts sont stockés dans un Firestore au lieu de les stocker en local ?
  - Pour le partage entre différents appareils et utilisateurs, mouais
- ACLs revus et JS dans les boosts désactivés par défaut
  - `<< We did an analysis of our Firebase access logs and confirmed that no creatorIDs had been changed outside those changed by the security researcher. >>`

https://kibty.town/blog/arc/

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

RCE chez Zimbra


CVE-2024-45519

- Plateforme d'hébergement de messagerie
  - Vulnérabilité du service *postjournal*
  - POC exécuté et efficace dans l'environnement car utilisateur authentifié et service activé
- Recommandation :
  - Vérifier si le service *postjournal* est activé (non par defaut)
  - Surveiller les utilisateurs dans la liste *mynetworks*
- Explication détaillée de l'exploitation dans le lien ci-dessous

https://blog.projectdiscovery.io/zimbra-remote-code-execution/

RCE sur Mario Kart 8 Deluxe sur Nintendo Switch


CVE-2024-45200

- Utilisation incorrecte de la librairie réseau Pia P2P lors d'une connexion LAN
  - POC présentant un débordement de tampon avec RCE et crash du jeu
  - Versions vulnérable : < v3.0.3

https://securityonline.info/kartlanpwn-cve-2024-45200-exploits-mario-kart-8-deluxe-lan-play-feature-for-rce/

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

RCE unauthenticated sur le plugin LittleSpeed Cache #WordPress

CVE-2024-44000

- Prise de contrôle de n’importe quel compte connecté
  - Celui d’un admin ? 🎁
- Causé par l’exposition du fichier */wp-content/debug.log*
  - Leak d’informations sensibles liées à l’authentification 🍪
- Utilisé sur 5 millions d’installations actives
- Affecte les versions ≤ 6.4.1
  - -- moins si la fonction de débogage est désactivée + debug.log supprimé

https://thehackernews.com/2024/09/critical-security-flaw-found-in.html

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

RCE unauthenticated pour LoadMaster


CVE-2024-7591

- 100 000 entreprises potentiellement vulnérables
- Equipements concernés : produits LoadMaster et Multi-Tenant Hypervisor de l'éditeur Kemp
- Versions concernées –>
  - **LoadMaster** : 7.2.60.0 et toutes les versions antérieures
  - **Multi-Tenant Hypervisor** : 7.1.35.11 et toutes les versions antérieures
- Patch non disponible pour le produit LoadMaster en version gratuite 

https://www.it-connect.fr/cette-faille-critique-dans-progress-loadmaster-pourrait-toucher-jusqua-100-000-entreprises/

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

Elévation de privilèges sur des produits Teamviewer

CVE-2024-7479
CVE-2024-7481

- Produits impactés : Remote Client et Remote Host
- Vérification incorrecte de la signature cryptographique (pour les deux failles)
  - Lors de l'installation des pilotes VPN et d'imprimantes
  - Possibilité d'installer un pilote malveillant (sans privilèges spécifiques)
- Passez sur les versions ≥ 15.58.4

https://securityonline.info/teamviewer-urges-users-to-patch-privilege-escalation-flaws-cve-2024-7479-and-cve-2024-7481/

Failles / Bulletins / Advisories
Réseau (principales failles)

RCE 0-click sur les chipsets Wi-Fi de MediaTek

CVE-2024-20017

- Chipsets Wi-Fi MT7622/MT7915 **et** bundles de pilotes RTxxx SoftAP
  - Bundles utilisés par Ubiquiti, Xiaomi et Netgear
  - MediaTek SDK ≤ 7.4.0.1 & OpenWrt 19.07 et 21.02 👋
- << Buffer overflow >> dans le démon **wappd**
- Patchs publiés en mars, PoC récemment publié

https://blog.sonicwall.com/en-us/2024/09/critical-exploit-in-mediatek-wi-fi-chipsets-zero-click-vulnerability-cve-2024-20017-threatens-routers-and-smartphones/

Faille critique dans pgAdmin

CVE-2024-9014

- Présente dans l'implémentation OAuth2
  - Identifiants codés en dur dans OAuth2 Authentication Handler
  - Permet le leak d'ID client et de secret
- Affecte les versions ≤ 8.11

https://securityonline.info/cve-2024-9014-cvss-9-9-pgadmins-critical-vulnerability-puts-user-data-at-risk/

Failles / Bulletins / Advisories
Autre (principales failles)

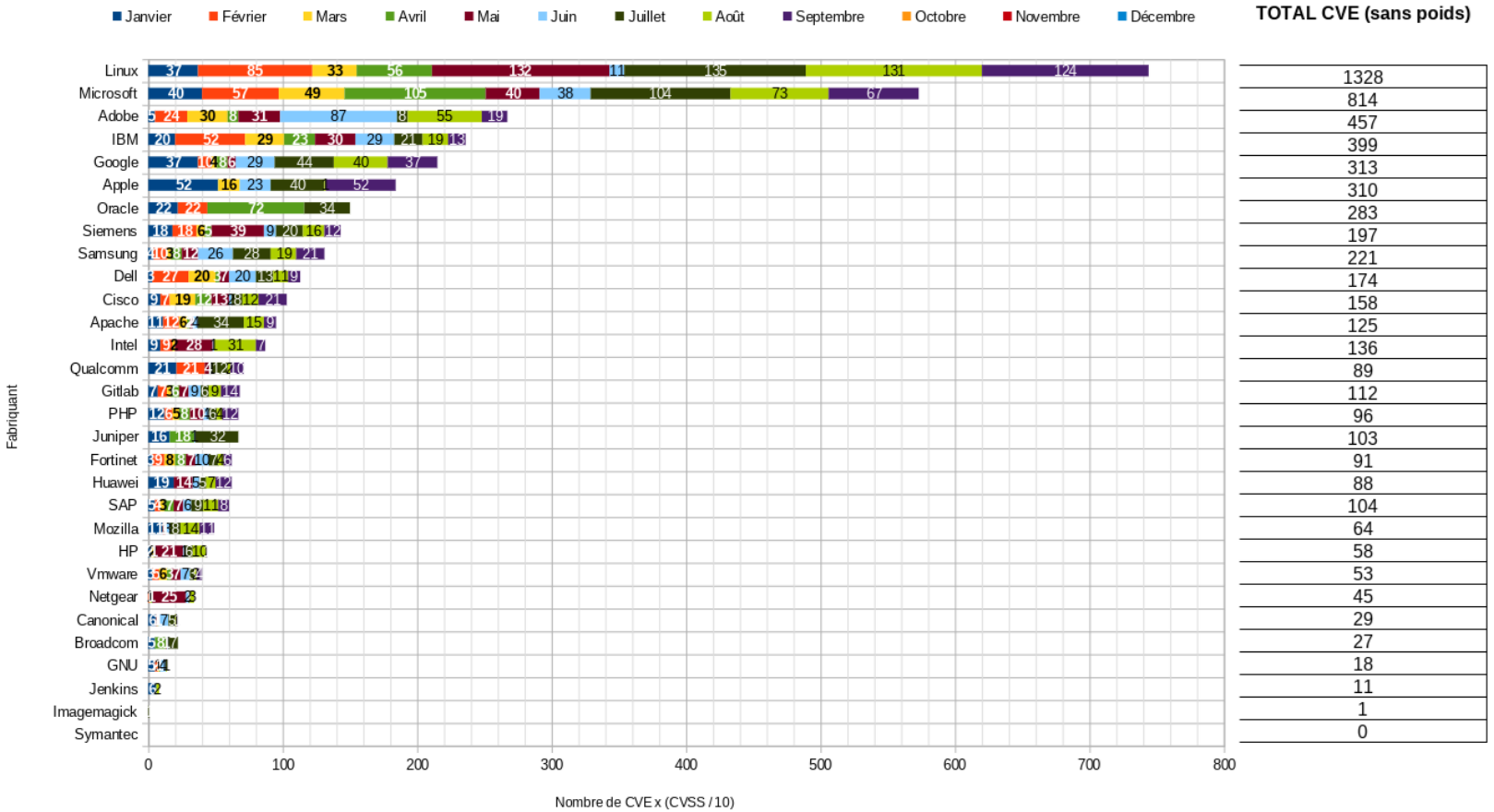
Prise de contrôle à distance de voitures Kia

- Il suffit **uniquement** de connaître la plaque d'immatriculation de la cible
  - Et de 30 secondes (lol)
- Failles permettant de déverrouiller les portes, les démarrer et les suivre à distance
  - Communication vers les systèmes de Kia en passant par l'infra dédiée aux concessionnaires
    - Avec possibilité de récupérer/modifier les informations personnelles des propriétaires
- Presque tous les véhicules fabriqués après 2013 impactés
  - Avec ou sans abonnement Kia Connect
- Correctif déployé mi-août par Kia
  - Aucune exploitation ne semble avoir été réalisée

https://samcurry.net/hacking-kia (liste des voitures impactées avec filtre par année et modèle)

https://www.usine-digitale.fr/article/cybersecurite-des-millions-de-vehicules-kia-exposes-un-piratage-a-distance.N2219630

Failles / Bulletins / Advisories
Stats du mois



TOTAL CVE (sans poids)
1328
814
457
399
313
310
283
197
221
174
158
125
136
89
112
96
103
91
88
104
64
58
53
45
29
27
18
11
1
0

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Malware

Infostealer pour Windows

- Corrigé par Windows dans le dernier patch
  - N'était pas sensé être exploité mais mise à jour récente
- Exploitable à l'aide de la vulnérabilité CVE-2024-38112
  - Corrigé par Windows en juillet 2024
  - Attaque de type spoofing sur la plateforme MSHTML, avec activation lors de la consultation d'un site web ou ouverture de fichiers
- Objectif : infecter les machines avec l'infostealer Atlantida
  - Attaque concentrée en Europe, Amérique du Nord et Asie Sud-Est

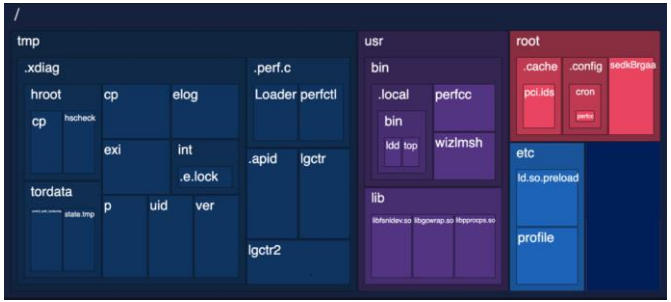
https://www.it-connect.fr/faille-windows-exploitee-pour-diffuser-un-malware-infostealer-cve-2024-43461/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Le malware Perfctl dans toute sa discrétion

- Malware Linux qui circule depuis 2021
  - Serait présent plusieurs milliers de machines !
- Roi de l'évasion et de la persistance
  - Suite à une infection : suppression du binaire + exécution en tâche de fond (service)
  - Propagation depuis la mémoire vers plusieurs répertoires du FS de sa cible
  - Exécution à chaque ouverture de session (~/.profile)
  - Manipulation de pcap_loop
  - Utilisation de relais Tor (externe) et de sockets (interne)
  - Kill de process gourmands quand l'utilisateur se connecte
- Privilégie l'exploitation de la CVE-2023-33426
  - Sinon il a encore 20k erreurs courantes à exploiter…
- Sert à miner ! #Monero et pas que :
  - Proxy-jacking, exfiltration de données, etc.

https://next.ink/152853/perfctl-un-malware-linux-tenace/



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

Temu : 87 000 000 de données

- Mise en vente de la base de données le 18/09 par smokinthashit
  - Contiendrai noms, identifiants, IP, date de naissance… hash de mots de passe
- Temu rétorque que ces données ne sont pas les tiennes
  - Le pirate affirme que le site Temu contient de nombreuses vulnérabilités
  - En attente de suite

https://www.it-connect.fr/temu-dement-existence-fuite-de-donnees-avec-87-millions-enregistrements/

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

Fortinet : 440 Go de données en vente

- Accès non autorisé sur un sharepoint chez Azure
  - Pas d’incident malveillant lié à l’incident
- Hacker “Fortibitch” indique avoir récupéré des données confidentielles
  - Contient des ressources pour les employés, des rapports financiers, de documents RH, des offres de produits, de rapports de vente, de services professionnels, de stratégies de marketing et d'informations sur les clients
  - Hacker appartient au cybergang DC8044

https://www.lemondeinformatique.fr/actualites/lire-fortinet-admet-qu-un-pirate-lui-a-vole-400-go-de-donnees-94704.html

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

Cultura, Boulanger, GrosBill, Truffaut [, plein d'autres] et aussi l'Assurance retraite !

- Horrormar44 en est toujours à l'origine
  - Ce qu'il avait annoncé sur BreachForums était vrai
- Données de 370.000 bénéficiaires volées
  - Adresse mail, numéro de sécurité sociale et montant des ressources perçues
    - Les données ne seraient pas récentes (a déclaré l'organisme)
  - Aucune donnée bancaire ou relative à un paiement
- Portail en ligne PPAS visé

https://www.zdnet.fr/actualites/des-donnees-de-370-000-beneficiaires-de-lassurance-retraite-volees-397126.htm

Piratages, Malwares, spam, fraudes et DDoS
Pannes

DDoS Record pour Cloudflare

- + d’un centaine d’attaque pendant ce mois-ci
  - Record : 2 milliards de paquets par seconde et 3.8 Tb/s (durée 65 secondes)
  - Secteurs visés : finances, Internet et télécommunication
- Attaquants venant de Vietnam, Russie, Brésil, Espagne et États-Unis
  - Attaque sur couche 3 et 4 avec protocole UDP sur un port fixe
  - Utilisation de routeurs ASUS utilisés par les particuliers, des équipements MikroTik, des enregistreurs DVR, ou encore des serveurs Web

https://www.it-connect.fr/cloudflare-bloque-une-attaque-ddos-record-pic-a-38-tbps/

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

Red Team Moteur de recherche de bypass de CSP

- Objectif : obtenir une XSS sur le site final
- Outil : https://cspbypass.com/

https://x.com/renniepak/status/1841495174729314352

Red Team Cloner facilement (et gratuitement) une voix (en CLI)

- Entrée : lui donner à manger un court clip audio du locuteur de référence
- Sortie : voix clonée avec les configurations souhaitées
  - Contrôle sur les émotions renvoyées, l'accent utilisé, le rythme, etc.
- Outil : https://github.com/myshell-ai/OpenVoice

https://research.myshell.ai/open-voice

DFIR / OSINT
Techniques & outils

Bellingcat : son gitbook ultime

- ONG mondialement connue spécialisée dans l'OSINT
- (énorme) Toolkit partagé !
  - Dans le cadre de la bourse 2024 Nieman-Berkman Klein
  - Classeur (Drive) → Gitbook : https://bellingcat.gitbook.io/toolkit
- 130 outils répartis dans plusieurs catégories
  - Imagerie satellite, analyse des réseaux sociaux, archivage de pages web, etc.

https://www.bellingcat.com/resources/2024/09/24/bellingcat-online-investigations-toolkit/

Business et Politique

Business
Monde

Google VS Microsoft : la bataille du Cloud

- Plainte de Google envers Microsoft pour pratiques anti-concurrentielles
  - Conditions de licence logiciels contraignent à rester chez Azure…
  - … ou une alternative d'une majoration de 400 %
- Dernière plainte en 2023 sans suite et conclu par un accord à l'amiable
- Microsoft subit de régulières plaintes de pratiques anti-concurrentielles avec Windows Server, Teams…

https://www.lefigaro.fr/secteur/high-tech/concurrence-google-cloud-porte-plainte-contre-microsoft-aupres-de-bruxelles-20240925

Droit / Juridique / Politique
Monde

Kaspersky → UltraAV

- Plus de MAJ depuis le 9 septembre
- Message aux clients indiquant une continuité d'activité passant par la solution UltraAV de la compagnie Pango
  - Surprise de désinstallation de Kaspersky et remplacement automatique par UltraAV
  - Utilisateurs mécontents et non rassuré par ces actions

https://www.it-connect.fr/aux-etats-unis-kaspersky-se-desinstalle-et-installe-ultraav-sans-avertissement/

Droit / Juridique / Politique
Monde

Durcissement de politique chez Telegram

- Pavel Durov, toujours en attente de son procès, annonce une collaboration de Telegram avec les autorités
  - Renforcement de l'équipe de modération afin de bloquer les résultats avec des mots-clés comme armes ou drogues
  - Divulgation des IP et des numéros de téléphone en réponse à des réquisitions judiciaires faites dans les règles

https://www.lemonde.fr/pixels/article/2024/09/23/pavel-durov-le-patron-de-telegram-annonce-un-durcissement-de-la-moderation_6330258_4408996.html

Droit / Juridique / Politique
Monde

Un membre d'Evil Corp tombe

- << Membre clé >> du groupe identifié
  - Viktorovich Ryzhenkov aka Beverley 🇷🇺
  - Evil Corp = filiale de LockBit
- Lié à plus de 60 opérations avec LockBit
  - 100 millions de $ extorqués
- Démasqué grâce aux données obtenues #Cronos
  - Grand succès !
- Chargé par le FCDO, l'OFAC et la DFAT

https://cybersecuritynews.com/authorities-unmasked-lockbit-affiliate/

https://next.ink/152662/le-demantelement-du-rancongiciel-lockbit-revele-ses-liens-avec-des-membres-du-gang-evil-corp/

Conférences

Conférences

Passée(s)

- **FranSec**, 10 septembre 2024 à Paris
- **Hexacon**, 04 au 05 octobre 2024 à Paris

À venir

- **Les Assises**, 09 au 12 octobre 2024 à Monaco
- **Unlock your Brain**, 08 au 09 novembre à Brest
- **Identity Days**, 22 novembre à Paris
- **Hackvens**, 22 novembre 2024 à Lille

Divers / Trolls velus

Divers / Trolls velus

Depreciation Windows Server Update Services

- Plus de WSUS dans la version 2025 de Windows Server
  - Plus de nouvelles fonctionnalités mais MAJ toujours présentes
  - Recommande de passer sur une version cloud comme Windows Autopatch

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-server-update-services-wsus-deprecation/ba-p/4250436

Que se passe-t-il si on intercepte le trafic d'un Pixel 9 Pro XL ?

- Données envoyées à Google toutes les 15 minutes
  - Adresse mail, n° de téléphone, localisation, liste des applications installées, état de la connexion, etc.
  - Envoyées entre autres à Device Management et Policy Enforcement
- La recherche vocale se connecte périodiquement aux serveurs de Google
- L'appareil tente de récupérer régulièrement de nouvelles mises à jour
  - Y compris auprès de serveurs appartenant à des environnements de test 😱

https://www.01net.com/actualites/toutes-15-minutes-pixel-9-envoie-donnees-google.html

FIN

Prochaine réunion ?

- RDV le **mardi 12 novembre 2024**

Accéder aux différents supports ?

Replays

Slides

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

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