Revue d'actualité de l'OSSIR

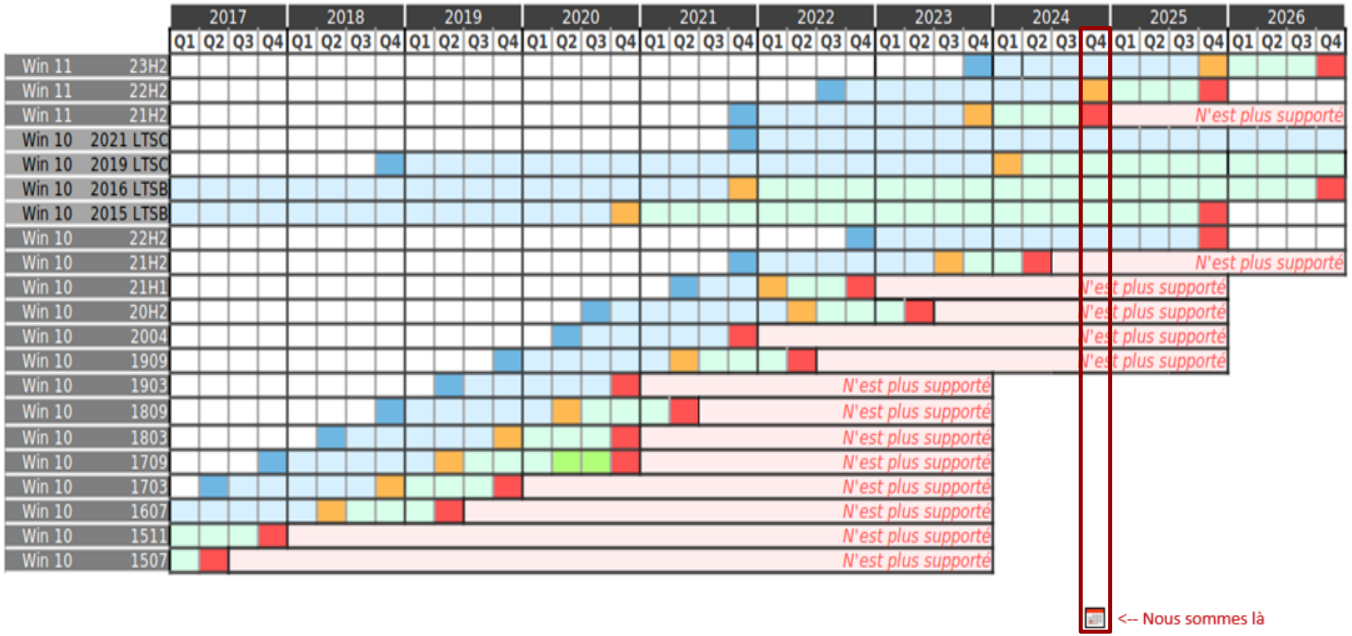
12 novembre 2024

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***



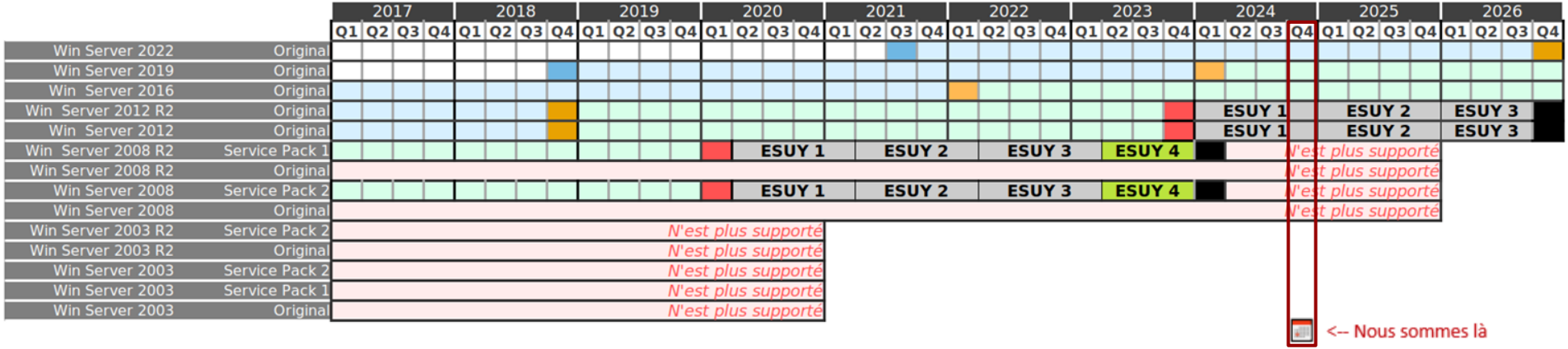
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



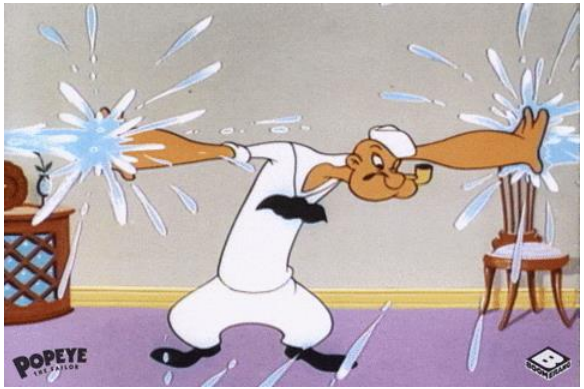
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 d'octobre, 118 vulnérabilités patchées dont

- 5 vulnérabilités de type 0-day :
  - [**CVE-2024-43573**] Windows MSHTML, spoofing
    - Bypass du correctif du mois dernier…
    - Affecte Windows 10 - 11 & Windows Server ≥ 2012 R2
  - [**CVE-2024-43572**] Microsoft Management Console, RCE
    - Ouverture de fichiers MSC malveillants
    - Affecte Windows 10 - 11 & Windows Server ≥ 2008 R2
  - [**CVE-2024-6197**] curl (libcurl), RCE
    - Via l'utilisation d'un certificat TLS malveillant
    - Affecte Windows 10 - 11 & Windows Server ≥ 2019
  - [**CVE-2024-20659**] Hyper-V, bypass de l'UEFI
    - Affecte Windows 10 - 11 & Windows Server ≥ 2019
  - [**CVE-2024-43583**] Winlogon, élévation de privilèges
    - Risque atténué si vous utilisez un IME (Microsoft)
    - Affecte Windows 10 - 11 & Windows Server ≥ 2008 R2
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2024-43468**] Microsoft Configuration Manager, RCE
  - [**CVE-2024-43488**] Visual Studio Code, RCE via l'extension pour Arduino
  - [**CVE-2024-43582**] Protocole RDP, RCE

https://www.it-connect.fr/microsoft-patch-tuesday-octobre-2024-recapitulatif/

Failles / Bulletins / Advisories
Systèmes

Ivanti Connect Secure RCE authenticated via CRLF injection


CVE-2024-37404

- Prérequis : avoir un accès admin sur le site web
  - Permet d'exécuter des commandes root sur le système
  - Vulnérabilité lors de la création d'une CSR
- Mise à jour vers ICS version 22.7R2.1, 22.7R2.2 ou Ivanti Policy Secure 22.7R1.1
- POC disponible

https://blog.amberwolf.com/blog/2024/october/cve-2024-37404-ivanti-connect-secure-authenticated-rce-via-openssl-crlf-injection/

Failles / Bulletins / Advisories
Systèmes

RCE 0-click unauthenticated sur NAS Synology Diskstation et BeeStation

CVE-2024-10443

- Découverte lors de la compétition Pwn2Own Ireland 2024
- Faille présente dans l'application Synology Photos (BeePhotos)
  - Non déployée par défaut sur les systèmes
- 90j pour mettre à jour les systèmes avant les détails techniques de l'exploitation
- Version patchée : Synology Photos 1.7 → 1.7.0-0795 ou supérieure
  Synology Photos 1.6 → 1.6.2-0720 ou supérieure
  BeeStation OS 1.1 → 1.1.0-10053 ou supérieure
  BeeStation OS 1.0 → 1.0.2-10026

https://www.it-connect.fr/synology-faille-de-securite-pwn2own-cve-2024-10443/

Failles / Bulletins / Advisories
Systèmes

Faille critique côté Fortinet

CVE-2024-23113

- Affecte FortiOS, FortiPAM, FortiProxy et FortiWeb
- << Format String >> dans le démon fgfmd de FortiOS
  - Permet une RCE unauthenticated

https://thehackernews.com/2024/10/cisa-warns-of-critical-fortinet-flaw-as.html?m=1

Version	Affected	Solution
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiPAM 1.3	Not affected	Not Applicable
FortiPAM 1.2	1.2 all versions	Migrate to a fixed release
FortiPAM 1.1	1.1 all versions	Migrate to a fixed release
FortiPAM 1.0	1.0 all versions	Migrate to a fixed release
FortiProxy 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiProxy 7.2	7.2.0 through 7.2.8	Upgrade to 7.2.9 or above
FortiProxy 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiWeb 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above

Failles / Bulletins / Advisories
Systèmes

Puis d’autres côté Palo Alto


CVE-2024-9463-66


CVE-2024-9467

- Affectent toutes les versions d’Expedition antérieures à la 1.2.96
- 5 CVEs :
  - [**CVE-2024-9463**] Injection de commande unauthenticated en tant que root
  - [**CVE-2024-9464**] Injection de commande en tant que root
  - [**CVE-2024-9465**] Injection SQL unauthenticated permettant de faire fuiter la base de données
  - [**CVE-2024-9466**] Exposition les identifiants et mots de passe du pare-feu et clés API
  - [**CVE-2024-9467**] XSS réfléchie

https://thehackernews.com/2024/10/cisa-warns-of-critical-fortinet-flaw-as.html?m=1

Failles / Bulletins / Advisories
Systèmes

Et également une côté CISCO

CVE-2024-20432

- Affecte leur NFDC (Nexus Dashboard Fabric Controller)
  - Versions comprises entre la 11.5 et 12.2.2 exclues
- Injection de commande depuis un compte à faibles privilèges
  - Directement depuis l’interface ou sinon via la REST API

https://thehackernews.com/2024/10/cisa-warns-of-critical-fortinet-flaw-as.html?m=1

Failles / Bulletins / Advisories
Navigateurs (principales failles)

Use-after-free dans Firefox (ESR)

CVE-2024-9680

- Bug dans le composant << Animation timeline >>
- Affecte :
  - Firefox 131.0.2
  - Firefox ESR 128.3.1 et Firefox ESR 115.16.1

https://thehackernews.com/2024/10/mozilla-warns-of-active-exploitation-in.html?m=1

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

Nouvelle vulnérabilité sur Bitcoin

- Possible de faire crasher des nœuds Bitcoins à distance
  - Si une erreur est générée lors de la réception d'un bloc → appel d'un message blocktxn
  - Attente d'une réponse mais réception d'une autre transaction pendant cette attente
  - Si une 2ème erreur de transaction est générée → 2ème message blocktxn
  - Résultat : crash du nœud
- Vulnérabilité corrigée en passant à la version 25.0

CVE-2024-35202

https://securityonline.info/bitcoin-core-vulnerability-cve-2024-35202-enables-remote-node-crashes/

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

Vulnérabilité critique sur Apache Solr

CVE-2024-45216

- Contournement de l'authentification avec le PKIAuthenticationPlugin
  - Activé par défaut
  - Une fausse fin d'URL de l'API ignore l'authentification et maintient le contrat d'API
- Version corrigée →
  - Apache Solr 5.3.0 avant 8.11.4
  - Apache Solr 9.0.0 avant 9.7.0

https://www.cvedetails.com/cve/CVE-2024-45216/

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

Elévation de privilèges dans Keycloak

CVE-2024-3456

- Se situe au niveau de la REST API
  - Nécessite un compte à faibles privilèges
  - Possibilité d’exécuter des commandes à plus haut niveau de privilège
- Vulnérabilité corrigée en passant à la version 24.0.5

https://securityonline.info/keycloak-patches-cve-2024-3656-granting-low-privilege-users-administrative-access/

Failles / Bulletins / Advisories
Smartphones (principales failles)

2 vulnérabilités Android

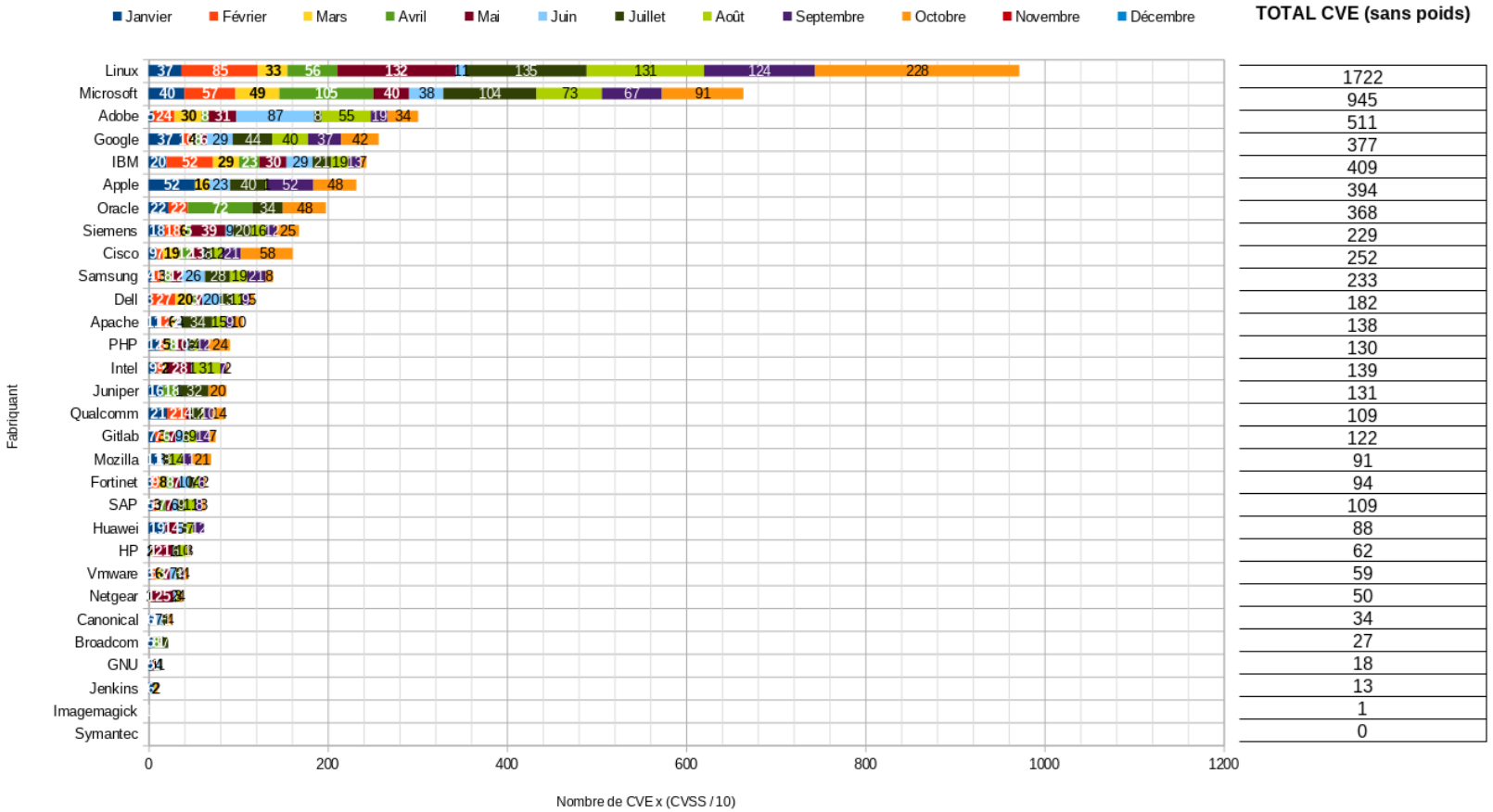

CVE-2024-43087

CVE-2024-43093

- 1ère : concerne les chipsets Qualcomm
  - Dans le protocole transférant des données dans le driver FastRPC
- 2ème : aucune information mais actuellement exploitée dans la nature
- Cible principale : appareils d'employés dans le but de voler les données d’entreprises

https://cyberscoop.com/2024-android-security-bulletin-november-qualcomm-fastrpc-driver/

Failles / Bulletins / Advisories
Stats du mois



TOTAL CVE (sans poids)
1722
945
511
377
409
394
368
229
252
233
182
138
130
139
131
109
122
91
94
109
88
62
59
50
34
27
18
13
1
0

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratages

Exploitation de cookies F5 Big-IP

- F5 Big-IP : ensemble d'application pour la gestion de trafic Web d'équilibrage de charge et de la sécurité, notamment grace au module Local Traffic Manager (LTM)
  - Module utilisant des cookies non chiffrés, permettant de connaître des serveurs cachés et ainsi analyser leurs vulnérabilités
- Nouvelle option << Obligatoire >> disponible pour le chiffrement des cookies depuis v11
- Mise en place aussi d'une solution d'analyse de configuration : Big-IP iHealth par F5
- Vulnérabilité connue et exploitée depuis quelques années selon le CISA

https://www.bleepingcomputer.com/news/security/cisa-hackers-abuse-f5-big-ip-cookies-to-map-internal-servers/

Piratages, Malwares, spam, fraudes et DDoS
Malware

Installation de malware via des paquets NPM douteux

- Processus d'audit et de vérification en place, mais insuffisants
  - Typosquatting toujours possible (noms très similaire à des bibliothèques existantes)
  - Injection de scripts malveillants
  - Obfuscation du code
  - Supply chain attack
- Vérifiez les dépendances utilisées, sensibilisez vos développeurs, MCS, etc.

https://securite.developpez.com/actu/364442/Invasion-silencieuse-des-centaines-de-bibliotheques-malveillantes-publiees-sur-NPM-tentent-d-installer-des-malwares-sur-les-machines-des-developpeurs-pour-infiltrer-les-entreprises/ (exemple d'attaques en cours)

Piratages, Malwares, spam, fraudes et DDoS
Hack 2.0

0-day par IA

- Big Sleep (IA de Google spécialisé en recherche de vulnérabilité) découvre une stack buffer underflow 0-day sur SQLite
- Objectifs : pouvoir anticiper et corriger des failles le plus tôt possible

https://www.forbes.com/sites/daveywinder/2024/11/05/google-claims-world-first-as-ai-finds-0-day-security-vulnerability/

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

Buffet à volonté pour (presque) Free

- Données de + de 19 millions de ses abonnés
  - Incluent 5.11 millions d'IBAN !!!!!!!
- Leak en vente sur Breach et vendu pour 175k $
- Quels sont les risques ?
  - Usurpation d'identité - Prêts bancaires
  - Usurpation d'identité - Abonnements
  - Prélèvements frauduleux
  - Phishing

→ Surveillez votre compte bancaire avec attention !

https://www.it-connect.fr/piratage-de-free-les-donnees-personnelles-et-les-iban-des-clients-vendus-pour-161-000-euros/

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

2024 - 2 millions de mot de passe VPN dans la nature

- Appartiennent aux services Proton VPN, NordVPN, CyberGhost VPN…
  - Récupérer à partir d'infostealer sur les machines victimes, par force brute ou par phishing
  - Nombreux mots de passe faibles
  - Peuvent correspondre à des accès à l'administrateur de l'AD

https://www.it-connect.fr/vpn-2-millions-de-mots-de-passe-compromis-en-2024/

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

Nokia - Grosse quantitée de données

- Mise en vente d'informations confidentielles par IntelBroker par l'intermédiaire d'un tiers
  - Clés SSH, code source, clés RSA, connexions Bitbucket, comptes SMTP et webhooks
  - Informations éligibles uniquement pour les membres ayant une solide réputation sur BreachForums
- Prise de contact par CyberInsider pour confirmer l'intrusion chez Nokia
  - Aucune réponse pour le moment

https://cyberinsider.com/hacker-claims-sale-of-nokia-source-code-on-underground-forums/

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

Campagne massive qui cible les dépôts Git

- Campagne nommée **EMERALDWHALE**
- But ?
  - Siphonner les informations d'identification, cloner les dépôts privés, etc.
- 10k dépôts privés collectés
  - Et stockés sur un S3 (Amazon) appartenant à une victime antérieure
    - Contient pas moins de 15k informations d'identification volées
    - Il a depuis été supprimé par Amazon
- Protégez vos dépôts Git et l'accès à vos .git !

https://thehackernews.com/2024/11/massive-git-config-breach-exposes-15000.html?m=1

Piratages, Malwares, spam, fraudes et DDoS
Pannes

Perte de données chez Microsoft

- Logs de sécurité des équipements Microsoft perdus
  - Données du 2 au 19 septembre
  - Concerne les équipements Microsoft Entra, Sentinel, Defender for Cloud, et Microsoft Purview
  - Serait dû à un bug dans leur agent de monitoring
- Mise en place d’un support par Microsoft au besoin
- Nombreuses entreprises impactées mais pas de compensation annoncée

https://techcrunch.com/2024/10/17/microsoft-said-it-lost-weeks-of-security-logs-for-its-customers-cloud-products/

Piratages, Malwares, spam, fraudes et DDoS
Pirater les pirates

Sophos contre les pirates chinois

- Repousse des attaques depuis plusieurs années
  - Attaques Web sur portails d'administrations, attaques sur satellite Sophos, VPN, 0-day…
- Déploiement d'un implant en 2020 pour surveiller les groupes de cybercriminels
  - A permis d'identifier de nombreuses informations comme des injections SQL et des injections de commande notamment une RCE critique encore inconnue
- Sophos déclare avoir attrapé un acteur chinois << TStark >> mi-2020
- Association avec le Netherland's National Cyber Security Center pour saisir les serveurs hébergeant les domaines C2 de l'attaquant

https://www.securityweek.com/sophos-used-custom-implants-to-surveil-chinese-hackers-targeting-firewall-zero-days/

Piratages, Malwares, spam, fraudes et DDoS
Publication

Réponse forte de OpenAI suite à l'utilisation de son service

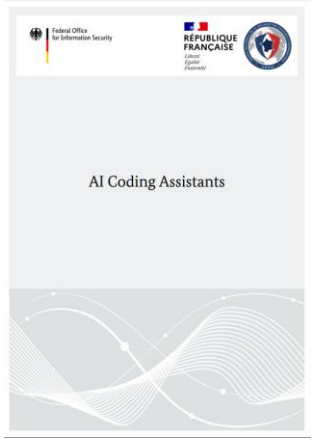
- Annonce d'un blocage d'une vingtaine de campagne
  - Permettant de faire le débogage de logiciels malveillants, la rédaction d'articles pour des sites web, la génération de biographies pour des comptes de médias sociaux et la création d'images de profil générées par l'IA pour de faux comptes sur X
- Nombreuses affaires mise en évidence
  - SweetSpecter, Cyber Av3ngers, Storm-0817, Tempête-2035…

https://thehackernews.com/2024/10/openai-blocks-20-global-malicious.html

Piratages, Malwares, spam, fraudes et DDoS
Publication

Nouveau rapport de l'ANSSI et de la BSI concernant l'IA

- Concerne plus exactement les risques liés aux assistants de programmation basés sur l'IA
  - Rapport conjoint entre l'Allemagne et la France
- Comment bien l'utiliser ?
  - Debugging, génération de tests (unitaires), revue de code, traduction vers un autre langage, etc.
- Quels sont les risques ?
  - Confidentialité du code !
  - << Automation Bias >> intéressant : l'humain risque de perdre en compétence
  - Faible qualité du code généré (et de sa sécurité)
- Bonnes pratiques présentes dans le rapport, allez y jeter un coup d'œil !



https://www.it-connect.fr/nouveaux-enjeux-de-securite-des-assistants-de-codage-ia-voici-le-rapport-de-lanssi-et-de-la-bsi/

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

Red Team Bypasser l'accès conditionnel d'Entra ID

- Accès défini par des règles basés sur plusieurs critères
  - Localisation, appareil, niveau de risque, etc.
- Outil nommé BAADTokenBroker
  - Utilisé pour de la post-exploitation
  - Authentification sur Entra ID via les clés stockés sur les machines compromises
    - Device key, Transport key, etc.

https://github.com/secureworks/BAADTokenBroker

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

Tester l'efficacité de votre solution adblock

- Outil : https://d3ward.github.io/toolz/adblock.html
- Tente de se connecter à plusieurs domaines liés à plusieurs catégories
  - Publicités, suivi de bogues, traqueurs sociaux, OEM, etc.
  - Liste en question : https://raw.githubusercontent.com/d3ward/toolz/master/src/d3host.txt
- Une version en ligne existe : https://d3ward.github.io/toolz/adblock.html

Business et Politique

Business
Monde

Quand Elon Musk joue avec le marché de l'IA

- xAI (entreprise d'Elon Musk) a mis en place un supercluster de 100k GPU en 19 jours
  - Technologie GPU utilisée : NVIDIA H200 Blackwell
  - Projet nommé Colossus
- Exploit qualifié de << surhumain >> par le PDG de Nvidia
  - Nécessite habituellement pas loin de 4 ans
- L'action de Nvidia a bondi de 14% au cours du mois d'octobre
- Superordinateur destiné à améliorer Grok (assistant de X) et la conduite autonome des Tesla

https://www.frandroid.com/marques/nvidia/2370724_elon-musk-reussit-une-prouesse-dans-ses-data-centers-meme-nvidia-nen-revient-pas

Business
Monde

Très lourde amende pour Google, peut-être même un peu trop

- Une amende de 20 décilions $ (rajoutez 33 x 0 derrière)
  - Réclamée par la Russie
  - Rappel : le PIB mondial est estimé à 100.000 milliards $
- Qu'est-ce qui leur est reproché ?
  - Avoir interdit la chaîne russe ultranationaliste Tsargrad en 2020
    - Ainsi que d'autres chaînes suite à l'invasion de l'Ukraine
  - 1025 $ d'amende qui double chaque semaine (ajoutez les intérêts)
- Google est inactif en Russie depuis 2022 donc pas besoin de trop s'inquiéter

https://www.theregister.com/2024/10/29/russian_court_fines_google/

Business
National

Une stratégie douteuse pour Atos qui se met à dos l'Etat français

- Prêt accordé en avril 2024 par Bercy (FDES)
- Les créanciers demandent à Atos deux choses
  - Convertir 3.1 milliards € d'emprunts et d'intérêts en capital pour alléger leur dette de 4 milliards
    - Validé par le tribunal du commerce
  - Transférer ses actifs français dans une double holding aux Pays-Bas
    - But : `<< réduire la fiscalité sur les plus-values de cessions d'actions et sur les dividendes >>`
- Suppression prévue de 400 postes en France d'ici 2 ans

https://www.capital.fr/entreprises-marches/atos-apres-avoir-recu-50-millions-de-bercy-le-groupe-cree-une-holding-fiscale-aux-pays-bas-1504556

Droit / Juridique / Politique
Monde

Zendesk ne reconnaît pas une vulnérabilité découverte

- Un adolescent trouve une vulnérabilité sur l'absence de vérification d'identité lors de l’envoi de ticket
  - Permet de faire du spoofing et de récupérer des informations confidentielles
- Le programme de bug Bounty de Zendesk ne prend pas en compte l’usurpation d'identité
  - Récompense de 0 $ pour l’adolescent
  - Zendesk discrédite l’adolescent pour actions illégales, violation de l'éthique et des CGU
- Récompense de 50.000 $ par plusieurs entreprises utilisant le service

https://securite.developpez.com/actu/363805/Un-adolescent-a-recu-0-de-Zendesk-et-50-000-des-clients-de-Zendesk-apres-avoir-divulgue-une-faille-de-securite-qui-a-expose-les-donnees-sensibles-de-ses-clients-du-Fortune-500/

Droit / Juridique / Politique
Monde

Retrait des mainteneurs russes du projet Linux (noyau)

- Retrait effectif lors de la publication du correctif du noyau Linux 6.12-rc4
  - https://github.com/torvalds/linux/blob/master/MAINTAINERS
- Linus Torvalds s'est exprimé dessus
  - `<< Je suis Finlandais. Vous pensiez que je soutiendrais l'agression russe ? >>`
  - Raison clairement politique
- Décision **définitive** selon Linus !

https://linux.developpez.com/actu/364099/Linus-Torvalds-s-est-exprime-au-sujet-du-retrait-des-mainteneurs-russes-de-la-liste-des-mainteneurs-de-pilotes-du-noyau-Linux-supposement-en-raison-de-leur-association-avec-la-Russie/

Droit / Juridique / Politique
Européen

L’AMF a parlé 🤦

- Rappel : DORA rentre en vigueur le 17 janvier 2025 (dans 3 mois !!!)
- Attentes révélées par la présidente au début du mois
  - 3 contrôles << SPOT >> effectués et résultats décevant :
    - `<< mauvaises pratiques et des insuffisances qui restent préoccupantes >>`
    - Procédures de contrôle répressives **promises**
  - Attentes similaires, quelque soit la taille de la structure
  - Gouvernance aussi importante que les mesures techniques
  - Ne pas innover au détriment de sa (cyber) sécurité
    - `<< je ne pense pas que le sérieux en matière de cybersécurité et de la protection des fonds et des données soit un obstacle à l’innovation >>`

https://www.linkedin.com/posts/daniel-kabangu-935691134_dora-amf-tpe-activity-7259932193630605315-poI_/

Droit / Juridique / Politique
Européen

Hello NIS2 🙋

- Rappel : NIS2 en vigueur depuis le 7 novembre 2024
- Mesures techniques de cyber sécurité ET de seuils pour qualifier les incidents importants à notifier à l'Autorité de Contrôle
- 11 types d’entités concernées
  - DNS,TLD, datacenter, cloud, CDN, moteur de recherche, infogérance…
- Amendes :
  - 10 millions € ou 2% du CA max pour entités essentielles
  - 7 millions € ou 1.4% du CA max pour entités importantes

https://www.linkedin.com/posts/marc-antoine-ledieu-a040917_nis2-entit%C3%A9s-et-r%C3%A9seaux-critiques-activity-7259444355919233024-KPI-

Opérations internationales

Opérations internationales

Frappe musclée d'Interpol : Operation Synergia II

- Démantèlement de 22.000 @ IP et + 1.000 serveurs utilisés pour des activités criminelles
  - Serveurs positionnés en Chine (Hong Kong et Macao) et en Mongolie
- Opération conjointe entre + 90 pays membres d'Interpol et de nombreux partenaires du secteur privé comme Trend Micro, Kaspersky…
  - 41 personnes arrêtées + 65 suspects
  - Saisie de 80 Go de données en Estonie correspondant aux serveurs de cybercriminels ainsi qu'une quarantaine d'équipements électronique

https://www.it-connect.fr/interpol-frappe-fort-22-000-adresses-ip-desactivees-1-000-serveurs-saisis/

Conférences

Conférences

Passée(s)

- **Les Assises**, 09 au 12 octobre 2024 à Monaco
- **Unlock your Brain**, 08 et 09 novembre à Brest

À venir

- **ECW**, 18 au 21 novembre à Rennes
- **Identity Days**, 22 novembre à Paris
- **Hackvens**, 22 novembre 2024 à Lille
- **Cloud & Cyber Security Expo**, 27 et 28 novembre à Paris
- **Trustech**, 03 au 05 décembre à Paris

Divers / Trolls velus

Divers / Trolls velus

MFA obligatoire chez Azure et Microsoft 365

- Phase 1 : MFA obligatoire pour compte admin depuis le 15 octobre
  - Portail Azure, au centre d'administration Microsoft Entra et au centre d'administration Intune
  - SMS sur téléphone, Microsoft Authenticator, clé de sécurité FIDO2
- Phase 2 pour début 2025
  - Azure CLI, Azure PowerShell, l'application mobile Azure et lors de l'utilisation des outils d'Infrastructure as Code (IaC)
- Période de grâce accordée par Microsoft sur demande pour retarder la mise en place du MFA jusqu’au 15 mars 2025

https://www.it-connect.fr/microsoft-mfa-obligatoire-portails-admins-octobre-2024/

Divers / Trolls velus

Arnaque grâce à DocuSign

- Souscription des pirates à un abonnement DocuSign
  - Donne accès à une solution d’eSignature grâce à une REST API
  - Permet la création de modèles et usurpation facilement l'identité d'autres marques. Par l'intermédiaire de l'API, ils sont parvenus à automatiser la création et l'envoi en masse de fausses factures
  - Détournement d’argent avec la facture signée de la victime

https://www.it-connect.fr/des-pirates-abusent-api-de-docusign-pour-envoyer-de-fausses-factures/

Divers / Trolls velus

La fin de RSA et d'AES ??? 😱😱😱

- Ce qui a été annoncé ?
  - Chiffrements cassés par un ordinateur quantique chinois
  - Fini SSL/TLS (entre autres) 😥
- Par qui ?
  - De gros (cyber) influenceurs (on ne va pas donner de noms)
- La réalité ?
  - Le nombre 2269753 (7 chiffres) a été factorisé = module RSA de 22 bits = RSA-22 cassé
    - Sauf qu'il est recommandé d'utiliser à minima RSA-2048 = nombre de 617 chiffres à factoriser (on est large)
  - L'ordinateur quantique utilisé, D-Wave Advantage, est canadien et accessible via le Cloud (pas 🇨🇳)
- Ce qui est drôle ?
  - On a fait mieux dans le passé :
    - RSA-332 cassé en 1991 : nombre de 100 chiffres décimaux
    - RSA-829 cassé en 2020 : nombre de 250 chiffres décimaux
  - Exploit réalisable et reproductible avec un cluster de 5 Raspberry Pi

https://www.linkedin.com/posts/boris-motylewski_les-chinois-ont-cass%C3%A9-rsa-activity-7254512554633256960-kKi1/
(excellent post LinkedIn qui dénonce la fake news)

Divers / Trolls velus

Un asPIRATEur pas très correcte !

- Aspirateur Deebot X2 Omni #Ecovacs
- La machine a commencé à proliférer des insultes racistes à son propriétaire
  - Sa paire identifiant / mot de passe était utilisée sur d'autres plateformes (credential stuffing)
  - Un attaquant l'a utilisé pour se connecter sur l'application Ecovacs et contrôler les hauts parleurs
    - Mais également la caméra et le contrôle à distance de l'aspirateur
- Faiblesses ?
  - Code PIN vérifié uniquement au niveau du client lourd
  - Son émis par la caméra pouvant être désactivé à distance (très utile pour ne pas prévenir le user)
- Cela aurait pu être pire…

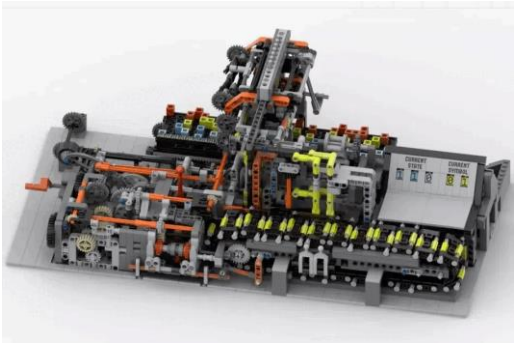
https://www.abc.net.au/news/2024-10-11/robot-vacuum-yells-racial-slurs-at-family-after-being-hacked/104445408

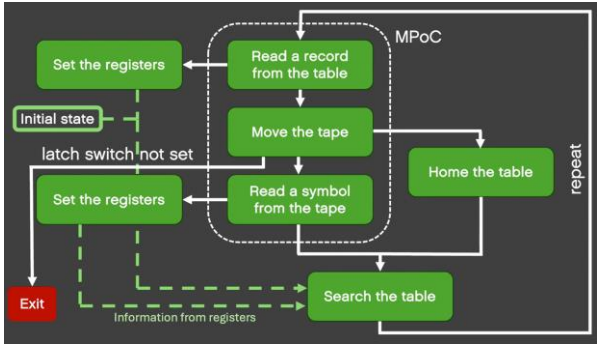
Divers / Trolls velus

Machine de Turing en … lego ?

- Machine totalement fonctionnelle !
  - Un ruban infini, une tête de lecture, plusieurs registres et un tableau de connexion
  - Instruction sur 7 bits
    - 3 pour l'état, 2 pour le symbole, 1 pour le déplacement gauche/droite et 1 pour l'arrêt
  - Aucun moteur électrique nécessaire, tout est mécanique
- 10.000 supporters, le projet passe maintenant en phase de revue
  - Plus d’infos en janvier 2025

https://ideas.lego.com/projects/10a3239f-4562-4d23-ba8e-f4fc94eef5c7





FIN

Prochaine réunion ?

- RDV le **mardi 10 décembre 2024**

Accéder aux différents supports ?

Replays

Slides

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

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