Revue d'actualité de l'OSSIR

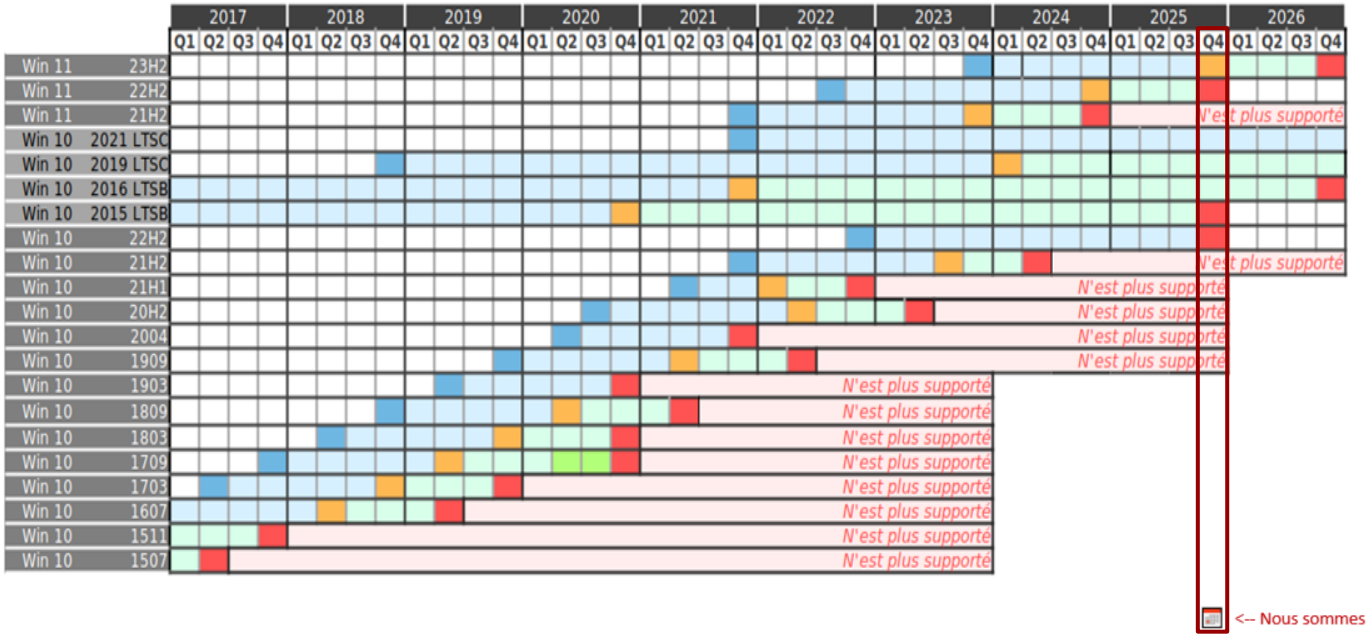
9 décembre 2025

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***



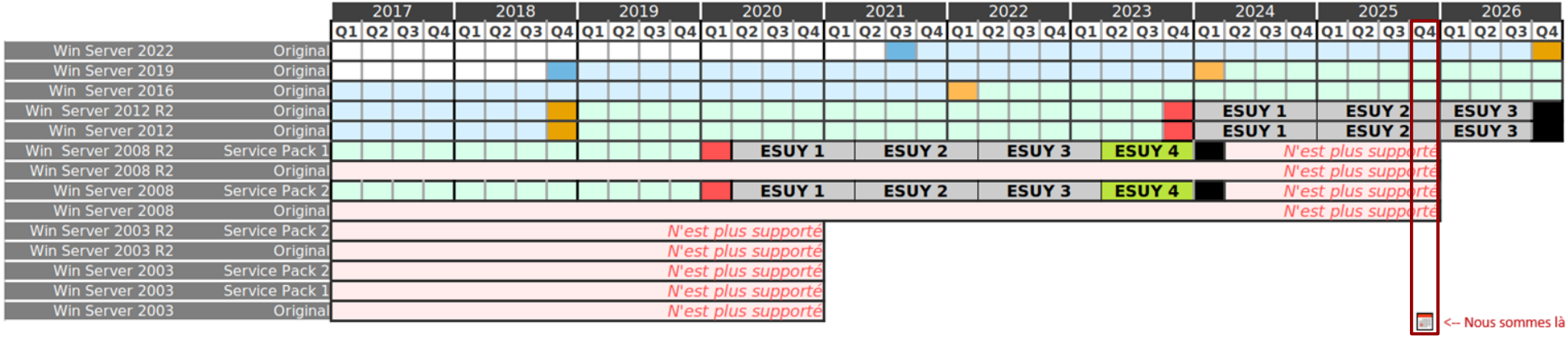
Sortie	Home, Pro	Entreprise
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13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



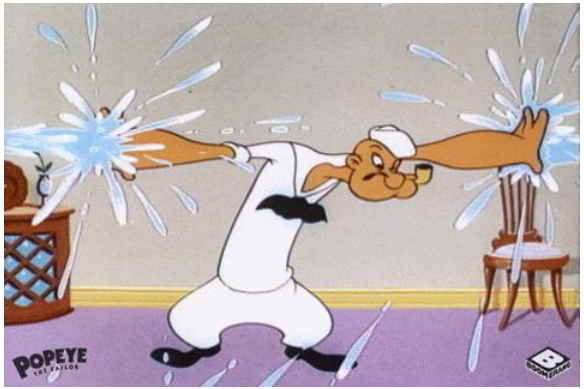
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre 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 novembre, 63 vulnérabilités patchées dont

- 1 vulnérabilité de type 0-day :
  - [**CVE-2025-62215**] Elévation de privilèges, noyau Windows
    - Type << Race Condition >>
    - Considérée comme complexe à exploiter
    - Affecte Windows 10 ≥ 1809 et Windows 11 & Windows Server ≥ 2019
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2025-62199**] RCE, Microsoft Office
  - [**CVE-2025-30398**] Leak d'informations, Nuance PowerScribe
  - [**CVE-2025-62214**] RCE, Visual Studio
  - [**CVE-2025-60716**] Elévation de privilèges, Windows DirectX
  - [**CVE-2025-60724**] RCE, Windows GDI+

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

Failles / Bulletins / Advisories
Système

Grafana, une faille pour être admin

CVE-2025-41115

- Située dans la fonctionnalité de provisioning SCIM
  - Est encore en << Public Preview >>, donc encore peu adoptée
  - Sert à provisionner et synchroniser automatiquement les utilisateurs et leurs attributs entre un fournisseur d'identité et des applications
- En modifiant l'id de l'utilisateur, permet d'usurper l'identité et de devenir administrateur par exemple
- Seules les versions Grafana Enterprise 12.0.0 à 12.2.1, avec SCIM activé, sont vulnérables
  - Aucune vulnérabilité sur les versions open source
  - Grafana Cloud, Amazon Managed Grafana et Azure Managed Grafana ont déjà eu les correctifs

https://www.it-connect.fr/grafana-scim-cve-2025-41115/

Failles / Bulletins / Advisories
Système

Faille liée aux fichiers raccourcis (.lnk) dans Windows


CVE-2025-9491

- Possibilité d'abuser massivement sur les ' ' dans le champ << Cible >>
  - Permettant de repousser la commande malveillante hors de la vue de l'utilisateur
- Faille remontée en mars 2025 par ZDI qui a été classée sans suite par MS
- ZDI remarque entre temps qu'il y a d'autres sujets :
  - Les .lnk autorisent une ligne de commande allant jusqu'à plusieurs dizaines de milliers de caractères
  - La fenêtre << Propriétés >> de Windows tronque l'affichage après 260 caractères
- La réalité ?
  - 11 groupes de pirates exploitent cette faiblesse depuis plusieurs mois
    - Evil Corp, Bitter, APT37, APT43, Mustang Panda, SideWinder, RedHotel, et Konni
  - Microsoft retire le troncage dans la fenêtre << Propriétés >>
    - Mais ne fait référence à ce changement dans aucun bulletin (???)

https://www.bleepingcomputer.com/news/microsoft/microsoft-mitigates-windows-lnk-flaw-exploited-as-zero-day/

Failles / Bulletins / Advisories
Système

0-day exploitée sur Fortinet

CVE-2025-64446

- Mise en lumière de la vulnérabilité début octobre par la société Defused
- Faille de type << Path Traversal >>
  - Permet à des attaquants non authentifiés de créer des comptes administrateurs sur les instances FortiWeb
- Patch disponible :

VERSION	VERSIONS AFFECTÉES	PATCH
FortiWeb 8.0	8.0.0 à 8.0.1	8.0.2 ou supérieur
FortiWeb 7.6	7.6.0 à 7.6.4	7.6.5 ou supérieur
FortiWeb 7.4	7.4.0 à 7.4.9	7.4.10 ou supérieur
FortiWeb 7.2	7.2.0 à 7.2.11	7.2.12 ou supérieur
FortiWeb 7.0	7.0.0 à 7.0.11	7.0.12 ou supérieur

- Recommandations si patch impossible :
  - Désactiver l'accès HTTP/HTTPS aux interfaces de gestion exposées sur Internet
  - Restreindre l'accès aux seules adresses IP de confiance
  - Surveiller les journaux pour repérer la création de nouveaux comptes administrateurs non autorisés
  - Contrôler la configuration à la recherche de modifications suspectes

https://www.it-connect.fr/fortinet-confirme-avoir-patche-une-faille-zero-day-dans-fortiweb-cve-2025-64446/

Failles / Bulletins / Advisories
Système

<< Command injection >> sur Fortinet


CVE-2025-58034

- Permet d'exécuter du code non autorisé sur le système via des requêtes HTTP ou des commandes CLI spécialement conçues
  - Prérequis : attaquant authentifié
- Exploitation active de la faille (+2.000 tentatives)
- Patch disponible :

VERSION	VERSIONS AFFECTÉES	PATCH
FortiWeb 8.0	8.0.0 à 8.0.1	8.0.2 ou supérieur
FortiWeb 7.6	7.6.0 à 7.6.5	**7.6.6** ou supérieur
FortiWeb 7.4	7.4.0 à 7.4.10	**7.4.11** ou supérieur
FortiWeb 7.2	7.2.0 à 7.2.11	7.2.12 ou supérieur
FortiWeb 7.0	7.0.0 à 7.0.11	7.0.12 ou supérieur

https://www.it-connect.fr/fortinet-cve-2025-58034-encore-une-faille-zero-day-dans-fortiweb/

Failles / Bulletins / Advisories
Navigateur (principales failles)

0-day dans le navigateur Chrome

CVE-2025-13223

- Type << Confusion >>
  - Présente dans le moteur JavaScript V8
  - Aucune autre information sur la faille
- Correctif intégré dans les versions suivantes :
  - Windows : 142.0.7444.175/.176
  - macOS : 142.0.7444.176
  - Linux : 142.0.7444.175

https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html

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

Faille sur WhatsApp qui a exposé des données de ses utilisateurs

- Possible d'extraire 3.5 milliards de n° de téléphone
  - Utilisation du système de découverte de contacts
    - 1) Enregistrer un à un tous les numéros de téléphone possibles
    - 2) Interroger l'interface Web de WhatsApp
    - 3) Identifier lesquels correspondent à un compte (et collecter les données)
  - Accès également possible à la photo de profil et au statut associé (quand il y en avait)
- Données de 54 millions d'utilisateurs français incluses
- Aucun mécanisme de rate-limit
  - Vulnérabilité déjà remontée à Meta en 2017 - aucune mesure corrective mise en place
  - Meta agit enfin en octobre 2025
    - Et considère que les données récupérées sont des `<< informations publiques basiques >>`
- Il est possible d'exposer son statut et sa photo de profil uniquement à ses contacts

https://www.it-connect.fr/cette-faille-whatsapp-a-expose-35-milliards-de-numeros-de-telephone/

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

React2Shell, le Log4Shell version 2025

CVE-2025-55182
CVE-2025-66478

- Faille présente dans React et Next.js
  - Exécution de code à distance, sans authentification requise
- Découverte dans le protocole Flight de RSC
  - `<< Tout framework ou bibliothèque intégrant l'implémentation react-server est susceptible d'être affecté. >>`
- 39% des environnements cloud contiennent des instances vulnérables (selon Wiz Research)
- Versions vulnérables :
  - React Server Components versions 19.0, 19.1.0, 19.1.1 et 19.2.0
  - Next.js : toutes les versions ≥ 15 et 16 & 14.3.0-canary.77
- PATCHEEEEEEEEZ

https://www.it-connect.fr/react2shell-vulnerabilite-react-nextjs-patchez-urgent/

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Smartube, mise à jour suspecte

- Application (mise à jour) bloquée sur Google Play Store
  - Clés de signature du développeur compromises
  - Revocation des clés
- Analyse de v30.51 - Mise en évidence d'une librairie inhabituelle *libalphasdk.so*
- Annonce du développeur de repartir sur une nouvelle application
  - Ancienne toujours valide mais plus de nouvelles mise à jour
- Recommandations :
  - Utiliser une version qui ne remonte pas d'alerte de Google (v30.19)
  - Désactiver les mises à jour automatiques
  - Changer le mot de passe de Google

https://www.it-connect.fr/smarttube-le-client-youtube-open-source-a-ete-pirate-une-mise-a-jour-suspecte-diffusee/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

EuroFiber France voit son système compromis

- Outil de ticketing compromis utilisé par des géants : Orange, Thales, SNCF…
- Intrusion le 13 novembre par le hacker ByteToBreach
  - Revendique avoir mis la main sur les informations de 10.000 entreprises, dont certains sensibles
  - Ainsi que des informations trés sensibles
    - Des configurations VPN, des mots de passe, des captures d'écran de systèmes internes, du code source, des certificats numériques et même des sauvegardes SQL
  - Rançon demandée pour non divulgation
- Vulnérabilité immédiatement corrigée chez EuroFiber
  - Selon eux, pas de données confidentielles exportées
- Affaire à suivre

https://www.clubic.com/actualite-587701-le-fournisseur-de-vpn-pro-de-thales-du-ministere-de-l-interieur-d-airbus-de-la-sncf-et-d-orange-se-fait-pirater.html

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Le logiciel médical Weda

- Fortement utilisé par les professionnels de santé
- Plateforme suspendue suite à une intrusion détecté le 10 novembre
  - Brèche colmatée + renforcement de la sécurité en cours
- Pas d'information sur une potentielle fuite de données encore
  - Critique car contient les dossiers médicaux des patients, leurs données de paiement, leurs cartes vitales…
- Affaire à suivre

https://www.01net.com/actualites/cyberattaque-inquietante-france-donnees-medicales-auraient-piratees-23-000-professionnels-sante-paralyses.html

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

Vol d'informations chez Logitech

- Vulnérabilité exploitée sur les serveurs Oracle (contenant la suite e-Business)
  - Patché en été, mais export des données
- Selon Logitech, pas de données personnelles
  - Contient des données internes sur clients, fournisseurs et collaborateurs
- Selon Clop, 1.8To de données exportés
  - Logitech a refusé de céder le chantage

https://www.01net.com/actualites/logitech-annonce-avoir-subi-une-fuite-de-donnees.html

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

Données de licenciés volés chez la FFF

- Compromission d'un compte d'un agent
  - A permis aux pirates de se connecter au logiciel de gestion administrative
- Mesures prises du côté de la FFF
  - Désactivation du compte compromis
  - Réinitialisant tous les mots de passe des comptes utilisateurs
- Type de données volées :
  - Nom, prénom, genre, date et lieu de naissance, nationalité, l'adresse postale, l'adresse mail, numéro de téléphone et numéro de licencié
- Mail envoyé aux personnes concernés
  - Indiquant que l'intrusion a été détectée le 20 novembre 2025

https://www.it-connect.fr/la-federation-francaise-de-football-fff-victime-dun-piratage-des-donnees-de-licencies-volees/

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

OpenAI et son prestataire Mixpanel

- Permet de collecter et analyser les interactions des utilisateurs avec l'interface principale de l'API d'OpenAI
  - Smishing le 9 novembre
  - Récupération d'informations : mail, localisation, OS, identifiants utilisateur
- Aucun système compromis chez OpenAI
  - Ni de mot de passe ou clé API compromis
- Fin de contrat avec le fournisseur
- Renforcement massive de la sécurité pendant ce temps chez Mixpanel

https://www.it-connect.fr/openai-chatgpt-une-fuite-de-donnees-chez-le-prestataire-mixpanel/

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

Fuite de données chez France Travail

- Données concernant 1.6 millions de jeunes suivis par le réseau des Missions locales
  - Noms, prénoms, identifiants France Travail, adresses mail / postale et n° de téléphone
  - Aucun mot de passe, aucune coordonnée bancaire
- Origine ?
  - Compromission du compte d'un responsable gestion de compte (d'une Mission locale)
    - Personne responsable des demandes d'habilitations au SI

https://www.it-connect.fr/nouvelle-fuite-de-donnees-chez-france-travail-les-donnees-de-1-6-million-de-jeunes-en-peril/

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

Un employé chez CrowdStrike un peu trop bavard

- Envoi de captures d'écran des systèmes internes à Scattered Lapsus$ Hunters
  - $ 25.000 promis
  - Il aurait également fournis des cookies SSO (révoqués rapidement)
- L'employé a évidemment été licencié
  - Et les autorités compétentes ont repris l'affaire
- N'oubliez pas que la menace peut venir de l'intérieur…

https://www.bleepingcomputer.com/news/security/crowdstrike-catches-insider-feeding-information-to-hackers/

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

Service Pajemploi de l'URSSAF

- Cyberattaque détecté le 14 novembre
  - 1.2 M de données de salariés
  - Nom, prénom, date et lieu de naissance, adresse postale, numéro de Sécurité sociale, nom de l'établissement bancaire, numéro Pajemploi et numéro d'agrément
- Pas de mail, IBAN, numéro de téléphone ou mot de passe

https://www.it-connect.fr/piratage-pajemploi-urssaf-jusqua-1-2-million-utilisateurs-affectes/

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

Crise chez Leroy Merlin

- Message reçu des clients d'une fuite de données
  - Nom, prénom, numéro de téléphone, adresse mail, adresse postale et date de naissance, ainsi que les informations liés au programme de fidélité
- Plainte déposée auprès de la CNIL

https://x.com/_SaxX_/status/1995898120039788610

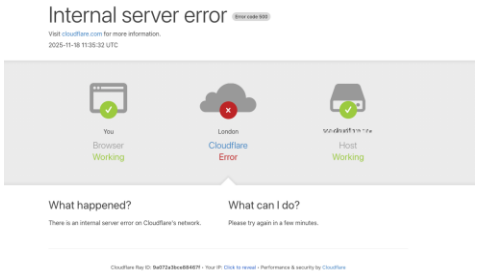
https://www.bfmtv.com/tech/cybersecurite/leroy-merlin-reconnait-avoir-ete-victime-d-une-cyber-attaque-et-annonce-que-des-centaines-de-milliers-de-clients-sont-concernes_AN-202512030877.html

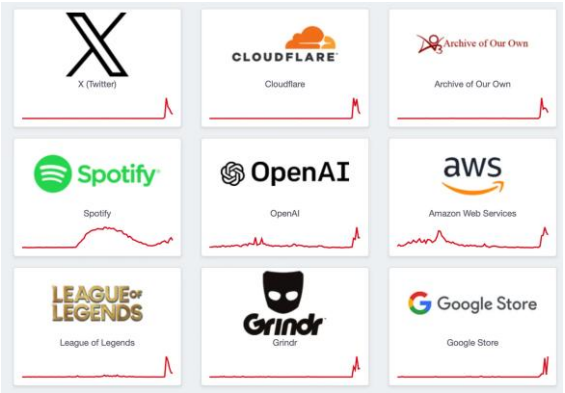
Piratages, Malwares, spam, fraudes et DDoS
Panne

Cloudflare est tombé, et 20% des principaux services web d'Internet avec lui

- À 11h20 UTC → défaillances majeures de transmission du trafic principal
- Cause ?
  - Un bug dans la logique de génération d'un fichier de configuration du module Bot Management
  - Ce fichier est devenu trop volumineux (double de la taille attendue) → plantage du système
- Les services internes de Cloudflare ont également été impactés
  - Tableau de bord, authentication via Turnstile, Workers KV, etc.
- À 17h06 UTC → tous les services de Cloudflare ont été restaurés

https://blog.cloudflare.com/fr-fr/18-november-2025-outage/



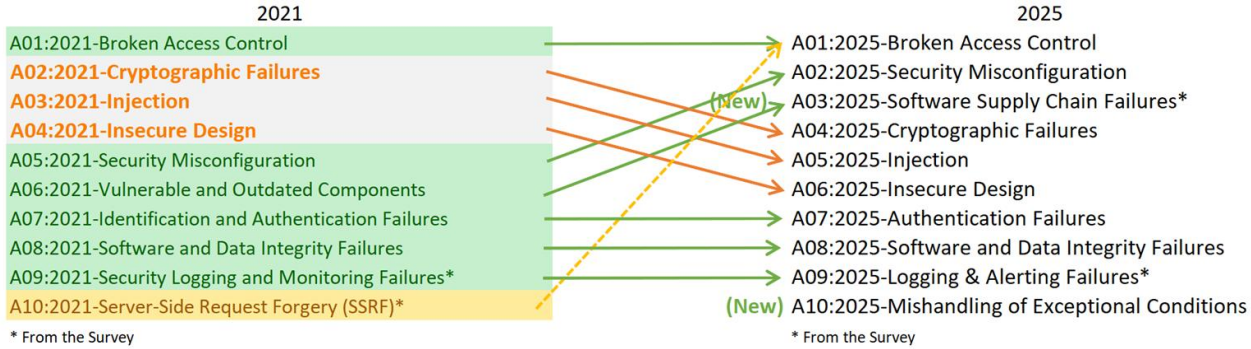


Piratages, Malwares, spam, fraudes et DDoS
Publication

Nouvelle version du TOP 10 OWASP : 2025 !

- Rappel :
  - 10 vulnérabilités web les plus critiques
  - Dernière version : 2021
- Changements à noter :
  - SSRF intègre la catégorie << Broken Access Control >>
  - Nouvelles catégories
    - << Mishandling of Exceptional Conditions >> → gestion incorrecte des erreurs
    - << Software Supply Chain Failures >> → défauts dans la chaîne d'approvisionnement logicielle

https://owasp.org/Top10/



Piratages, Malwares, spam, fraudes et DDoS
Technique & outil

Blue Team **Outil pour identifier si une adresse IP est malveillante ou pas**

- GreyNoise IP Check
- Vérification gratuite en quelques secondes
- Fait la distinction entre :
  - Les services inoffensifs
  - Les terminaux compromis
  - Les campagnes de reconnaissance actives
- Affiche une chronologie sur l'adresse IP interrogée sur 90 jours

https://check.labs.greynoise.io/

Business et Politique

Droit / Juridique / Politique
Europe

Digital Omnibus va tout changer ?

- Proposition de réforme du cadre réglementaire numérique de l'UE (19 novembre 2025)
- Principaux textes législatifs de l'UE impactés : RGPD, NIS2, DORA, eIDAS2, AI Act, etc.
- Deux volets principaux :
  - Volet << data / numérique >>
    - Révision ciblée de règles sur les données, la vie privée, la cybersécurité
    - Simplification et harmonisation de dispositions dispersées dans plusieurs textes existants
    - Allègement de certaines obligations jugées trop lourdes pour les entreprises
    - Exemple de mesure : notification d'incident cyber une seule fois via un point d'entrée unique
  - Volet << IA / technologie >>
    - Ajustements pour faciliter la mise en œuvre du AI Act
    - Réduction des charges administratives
    - Clarifications pour les développeurs et utilisateurs d'IA

https://ledieu-avocats.fr/omnibus-digital-proposal-ue-official-19-11-2025-avec-details-a-telecharger/

Conférences

Conférences

Passée(s)

- European Cyber Week (ECW), 17 au 20 novembre à Rennes
- GreHack, 28 au 29 novembre 2025 à Grenoble
- Trustech, 2 au 4 décembre 2025 à Paris

À venir

- JSSI, 10 mars à Paris
  - Sujet : << La Supply Chain, maillon faible de la Cyber >>
  - Appel à communications !

Divers / Trolls velus

Divers / Trolls velus

IACR, perte de la clé de déchiffrement

- Annulation des élections des dirigeants
  - Scrutin numérique à bulletin secret
  - Besoin de 3 clés de déchiffrement, remis à des personnes spécifiques
- Perte d'une des clés entraînant l'annulation des élections par un des chercheurs
  - Nouvelles élections le 20 décembre
  - Mise en place d'un nouveau procédé pour contrer ce genre de situation

https://www.courrierinternational.com/article/fiasco-des-cryptographes-de-renom-incapables-de-dechiffrer-les-resultats-d-un-scrutin-interne_237814

Divers / Trolls velus

Vengeance et reset de mot de passe

- Licenciement d'un employé en 2021
- Usurpation d'identité d'un autre employé pour obtenir de nouveaux identifiants de connexion
  - Connexion et exécution d'un script Powershell, réinitialisant tous les mots de passe (2.500)
- Risques : jusqu'à 10 ans de prison + amende max de 250.000 $ pour fraude informatique.

https://www.numerama.com/cyberguerre/2125059-contrarie-par-son-licenciement-il-seme-la-zizanie-et-modifie-les-mots-de-passe-de-2500-collegues.html

Divers / Trolls velus

1Password et Bitwarden maintenant intégrés à Windows 11

- But : stocker les clés d'accès des applications de manière sécurisée
- *Paramètres > Comptes > Clés d'accès > Options avancées*
  - 1Password déjà proposé
  - Bitwarden proposé en version bêta
- Vers une fin des mots de passe ? Oui.

https://www.frandroid.com/marques/microsoft/2864637_microsoft-integre-nativement-1password-et-bitwarden-a-windows-11-pour-en-finir-avec-les-mots-de-passe

Divers / Trolls velus

La fin de KMS ? Oui, mais de KMS38

- Méthode très ancienne utilisée pour l'activation offline de Windows (et d'Office)
  - Désactivée par Microsoft via la mise à jour KB5068861 (pour Windows 11 24H2/25H2)
- Comment ?
  - Outil *gatherosstate.exe* supprimé
    - Destiné initialement pour aider à la migration des licences KMS
    - Adieu les licences qui se terminaient (artificiellement) en 2038 👋
- Massgrave répond avec la version 3.8 de l'outil, nommée << R.I.P.KMS38 >>
  - Nouvelles techniques : HWID et TSforce
  - Connexion Internet nécessaire (besoin de se connecter auprès des serveurs MS)

https://lecrabeinfo.net/actualites/fin-de-kms38-microsoft-bloque-la-celebre-methode-dactivation-hors-ligne-de-windows/

FIN

Prochaine réunion ?

- RDV le **mardi 13 janvier 2026**

Accéder aux différents supports ?

Replays

Slides

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

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


L’équipe OSSIR
vous souhaite
de belles fêtes
de fin d’année !