Revue d'actualité de l'OSSIR

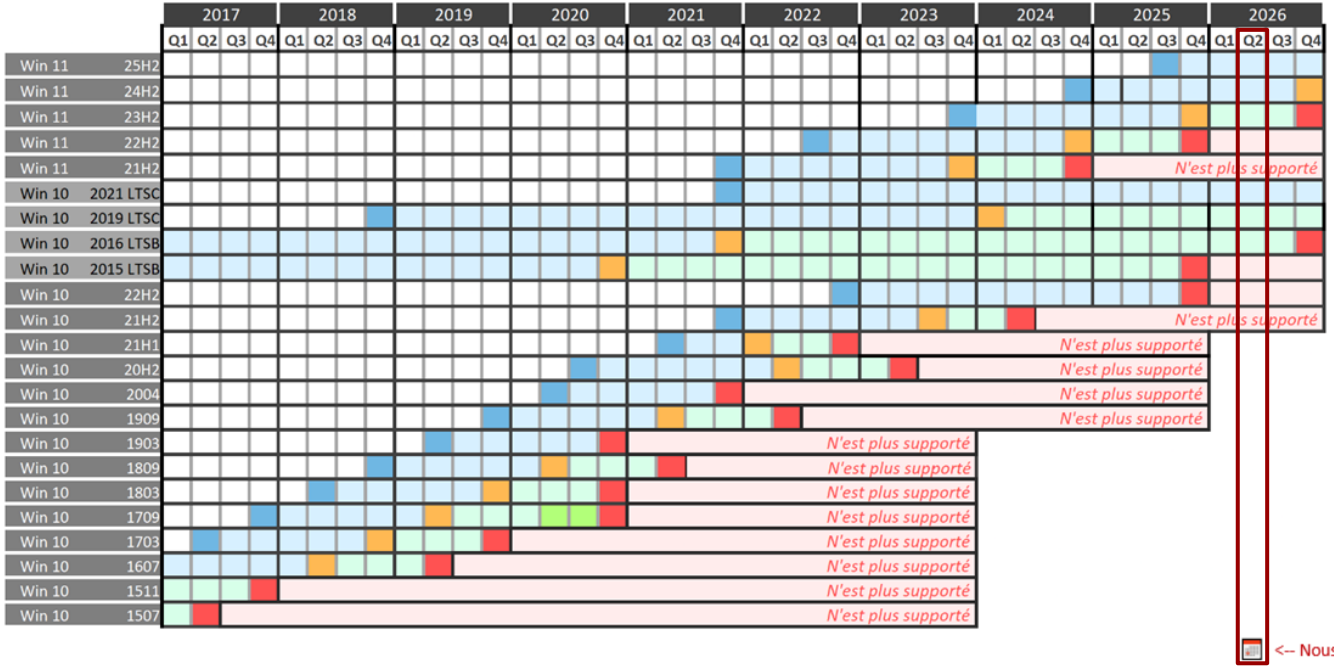
14 avril 2026

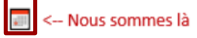
Jérémy De Cock
Melchior Courtois

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

Rappel du support Windows en couleurs

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





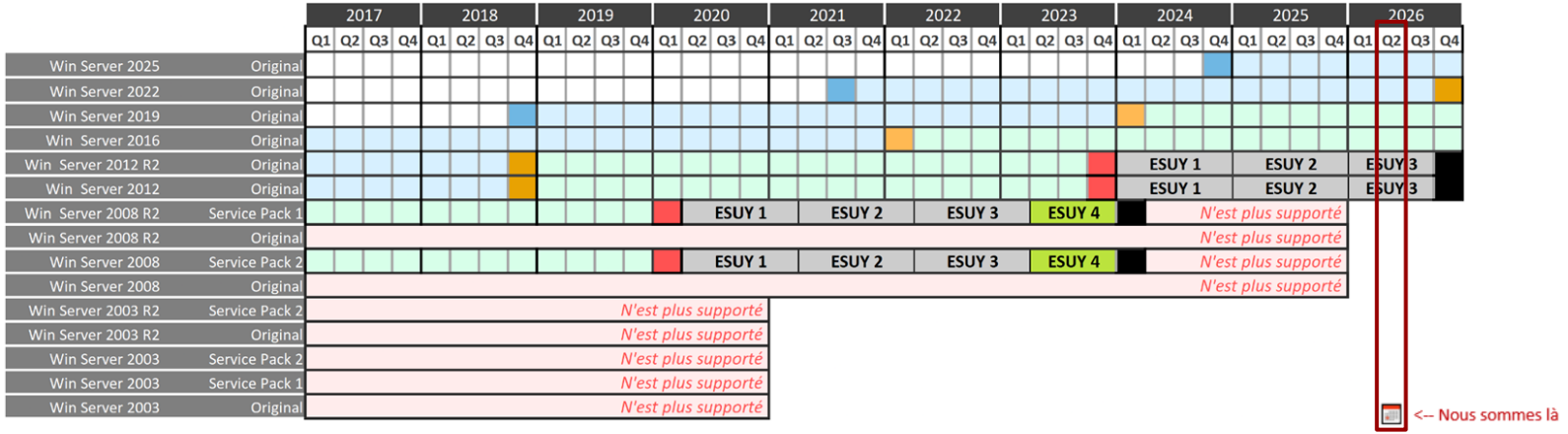
Sortie	Home, Pro	Entreprise
mardi 30 septembre 2025	mardi 12 octobre 2027	mardi 10 octobre 2028
mardi 1 octobre 2024	mardi 13 octobre 2026	mardi 12 octobre 2027
mardi 31 octobre 2023	mardi 11 novembre 2025	mardi 10 novembre 2026
mardi 20 septembre 2022	mardi 8 octobre 2024	mardi 14 octobre 2025
lundi 4 octobre 2021	mardi 10 octobre 2023	mardi 8 octobre 2024
mardi 16 novembre 2021	mardi 12 janvier 2027	mardi 12 janvier 2027
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029
mardi 2 août 2016	mardi 12 octobre 2021	mardi 13 octobre 2026
mercredi 29 juillet 2015	mardi 13 octobre 2020	mardi 14 octobre 2025
mardi 18 octobre 2022	mardi 14 octobre 2025	mardi 14 octobre 2025
mardi 16 novembre 2021	jeudi 13 juillet 2023	mardi 11 juin 2024
mardi 18 mai 2021	mardi 13 décembre 2022	mardi 13 décembre 2022
mardi 20 octobre 2020	mardi 10 mai 2022	mardi 9 mai 2023
mercredi 27 mai 2020	mardi 14 décembre 2021	mardi 14 décembre 2021
mardi 12 novembre 2019	mardi 11 mai 2021	mardi 10 mai 2022
mardi 21 mai 2019	mardi 8 décembre 2020	mardi 8 décembre 2020
mardi 13 novembre 2018	mardi 10 novembre 2020	mardi 11 mai 2021
lundi 30 avril 2018	mardi 12 novembre 2019	mardi 10 novembre 2020
mardi 17 octobre 2017	~~9 avril~~ 4 sept. 2019	~~14 avril~~ 13 oct. 2020
mercredi 5 avril 2017	mardi 9 octobre 2018	mardi 8 octobre 2019
mardi 2 août 2016	mardi 10 avril 2018	mardi 9 avril 2019
mardi 10 novembre 2015	mardi 10 octobre 2017	mardi 10 octobre 2017
mercredi 29 juillet 2015	mardi 9 mai 2017	mardi 9 mai 2017

Légende :

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

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

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



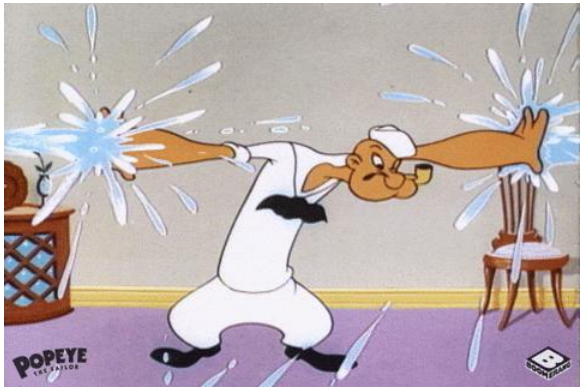
Sortie	Standard	LTSB/LTSC	Extension(s)
mercredi 18 août 2021	mardi 13 octobre 2026	mardi 14 octobre 2031	
mardi 13 novembre 2018	mardi 9 janvier 2024	mardi 9 janvier 2029	
samedi 15 octobre 2016	mardi 11 janvier 2022	mardi 12 janvier 2027	
lundi 25 novembre 2013	mardi 9 octobre 2018	mardi 10 octobre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

Légende :

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

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

Failles / Bulletins / Advisories



Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de février, 59 vulnérabilités patchées dont

- 6 vulnérabilités de type 0-day :
  - [**CVE-2026-21510**] Bypass des fonctions de sécurité Win, Windows SmartScreen et Windows Shell
    - Affecte Windows 10 et 11 & Windows Server 2012 à 2025
  - [**CVE-2026-21513**] Bypass des fonctions de sécurité Win, Framework MSHTML
    - Permet d'exécuter du code sur la machine
    - Affecte Windows 10 et 11 & Windows Server 2012 à 2025
  - [**CVE-2026-21514**] Bypass des fonctions de sécurité Win, Microsoft Word
    - Concerne les mesures d'atténuation OLE contre les contrôles COM/OLE malveillants
    - Affecte Microsoft 365 Apps for Enterprise & Office LTSC 2021/2024 pour Windows et Mac
  - [**CVE-2026-21519**] Elévation de privilèges, Gestionnaire de fenêtres du bureau
    - Affecte Windows 10 et 11 & Windows Server 2016 à 2025
  - [**CVE-2026-21525**] Déni de service, Gestionnaire de connexion à distance
    - Affecte Windows 10 et 11 & Windows Server 2012 à 2025
  - [**CVE-2026-21533**] Elévation de privilèges, Services de bureau à distance
    - Exploitée dans la nature (localement) pour ajouter un nouvel utilisateur dans le groupe Admins #CrowdStrike
    - Affecte Windows 10 et 11 & Windows Server 2012 à 2025
- Elles ont toutes été ajoutées au catalogue KEV de la CISA

https://www.it-connect.fr/patch-tuesday-fevrier-2026-recapitulatif/

Failles / Bulletins / Advisories (MMSBGA)
Microsoft

Bulletin de mars, 84 vulnérabilités patchées dont

- 2 vulnérabilités de type 0-day :
  - [**CVE-2026-21262**] Elévation de privilèges, SQL Server
    - Permet de devenir SQLAdmin sur un réseau
    - Affecte SQL Server 2016, 2017, 2019, 2022 et 2025
  - [**CVE-2026-26127**] Déni de service, .NET
    - Provoquée par une lecture hors limites
    - Affecte :
      - .NET 9.0 et 10.0 sur Windows, macOS et Linux
      - Microsoft.Bcl.Memory 9.0 et 10.0
- Les plus critiques ou les plus intéressantes :
  - [**CVE-2026-26144**] Information disclosure, Microsoft Excel
  - [**CVE-2026-26110|26113**] RCE, Microsoft Office

https://www.it-connect.fr/patch-tuesday-de-mars-2026-microsoft-corrige-84-failles-dont-2-zero-days/

Failles / Bulletins / Advisories
Système

La nouvelle faille Telnet

- Porté par le démon « `GNU InetUtils telnetd` » et permet d'obtenir un accès root en une seule commande
  - Vulnérabilité exploitable à distance sans authentification
- Pas encore de patch disponible
- Recommandations :
  - Désactiver le service Telnet
  - Restreindre les privilèges (en enlevant les droits root)
  - Bloquer le port 23 au niveau de vos firewalls périmétriques et celui de l'hôte, pour empêcher tout accès externe non désiré
  - Restreindre l'accès Telnet à certaines adresses IP ou en passant par une connexion sécurisée

https://www.it-connect.fr/cve-2026-32746-les-serveurs-linux-menaces-par-une-nouvelle-faille-telnet/

CVE-2026-32746

Failles / Bulletins / Advisories
Système

On continue dans les accès root


CVE-2026-3888

- PrivEsc via le service snapd
  - Deux services en particulier : « `snap-confine et systemd-tmpfiles` »
- Difficulté d'exploitation car dépend du temps
  - S'exécute lors du roulement des fichiers temporaires

Version Ubuntu (Release)	Version de snap avec le patch
25.10 questing	2.73+ubuntu25.10.1
24.04 LTS noble	2.73+ubuntu24.04.1
22.04 LTS jammy	2.73+ubuntu22.04.1
20.04 LTS focal	2.67.1+20.04ubuntu1~esm1 *(Ubuntu Pro)*
18.04 LTS bionic	2.61.4ubuntu0.18.04.1+esm2 *(Ubuntu Pro)*
16.04 LTS xenial	2.61.4ubuntu0.16.04.1+esm2 *(Ubuntu Pro)*

https://www.it-connect.fr/cve-2026-3888-quand-le-nettoyage-systeme-dubuntu-offre-un-acces-root/

Failles / Bulletins / Advisories
Système

Patch disponible pour Ubiquity

CVE-2026-22557
CVE-2026-22558

- Corrige 2 failles de sécurité
  - Path Traversal sans authentification, permettant de compromettre l'instance UniFi
  - Injection NoSQL avec authentification, permettant d'élever ses privilèges
- Attaque combinée dévastatrice
- Patch → v10.1.89

https://www.it-connect.fr/ubiquiti-cve-2026-22557-cette-faille-critique-menace-votre-reseau-unifi/

Failles / Bulletins / Advisories
Système

Bon point pour Claude

CVE-2026-34714

- Identification d'une faille de sécurité sur Vim
  - Pas de vérification lors de l'utilisation de l'option `tabpanel`
  - Patch disponible → v9.2.0272
- Vulnérabilité identifiée ensuite sur emacs
  - Lié à l'intégration native avec les systèmes de contrôle de version (vc-git)
  - Lecture automatique du fichier `.git/config` lors de la décompression
  - Manipulation du paramètre `core.fsmonitor –>` exécution de code
  - Pas de patch car vulnérabilité au niveau de Git selon emacs

https://www.it-connect.fr/ia-claude-a-identifie-une-faille-rce-importante-dans-vim-et-emacs/

Failles / Bulletins / Advisories
Système

BlueHammer : exploit d'une 0-day ?

- Faille permettant d'obtenir les droits SYSTEM ! #LPE
- Exploit publié sur GitHub
  - Fiabilité remise en cause en raison de quelques bugs identifiés
  - Faiblesses exploitées : TOCTOU et path confusion
- Chercheur VS le MSRC de Microsoft
  - `« Contrairement aux fois précédentes, je n'explique pas comment cela fonctionne ; vous êtes des génies, vous trouverez bien par vous-mêmes. Un grand merci à la direction du MSRC pour avoir rendu cela possible. »`
- Résultat : une 0-day est dans la nature

https://www.bleepingcomputer.com/news/security/disgruntled-researcher-leaks-bluehammer-windows-zero-day-exploit/

Failles / Bulletins / Advisories
Système

Failles critiques chez Veeam

- 5 vulnérabilités corrigées dans Veeam Backup & Replication
  - Dont 3 critiques
- Failles présentes sur toutes les versions
  - Patch disponible → v13.0.1.2067

https://www.it-connect.fr/patch-mars-2026-veeam-backup-replication-5-failles-corrigees-dont-3-critiques/

CVE-2026-21669
CVE-2026-21708
CVE-2026-21671

CVE-2026-21672
CVE-2026-21670

Failles / Bulletins / Advisories
Système

Wordpress : +3 versions -10 failles

- 3 versions poussées en 48H afin de sécuriser et stabiliser
  - Failles de type path traversal, XSS, DoS, SSRF…
- Correction de ces failles avec un 1er patch → bug pouvant faire planter Wordpress
- 2ème patch de correction pour ce bug
  - Découverte que le 1er patch de sécu pas assez efficace
- 3ème patch de sécurité → v6.9.4

https://www.it-connect.fr/wordpress-10-failles-corrigees-et-3-versions-deployees-en-48h/

Failles / Bulletins / Advisories
Système

Faille critique sur Dell


CVE-2026-22769

- Concerne le RecoverPoint for Virtual Machines (RP4VM)
  - Fortement exploitée par le groupe UNC6201 depuis mi-2024 😱
- Identifiant hardcodé 😱 😱
  - Identifiant `admin` présent dans `/home/kos/tomcat9/tomcat-users.xml`
  - Déploiement d'un paquet puis exécution de commandes en root
  - Possible de compromettre toutes les machines virtuelles

https://www.it-connect.fr/dell-recoverpoint-faille-critique-cve-2026-22769/

Failles / Bulletins / Advisories
Système

Alertes du côté des solutions Citrix NetScaler 🚨

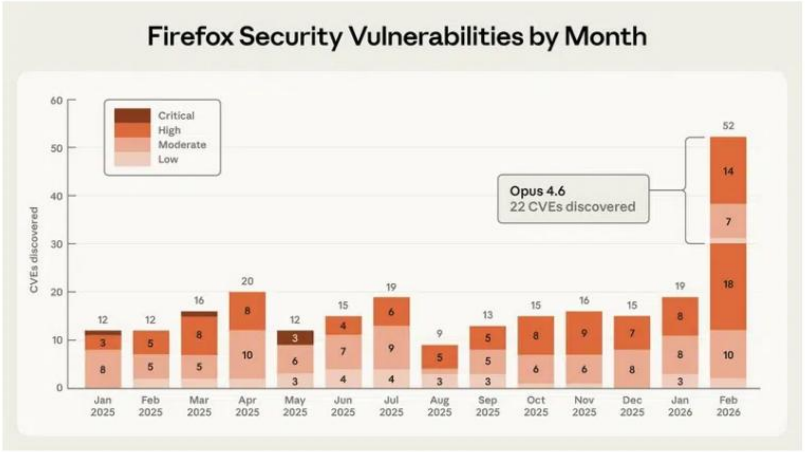
- 2 failles de sécurité :
  - [**CVE-2026-4368**] Race condition permettant de provoquer un mixage de sessions users
    - Et permettre d'usurper la session active d'un autre utilisateur
    - Affecte les appliances configurées en tant que passerelles ou serveurs virtuelles AAA
  - [**CVE-2026-3055**] Validation insuffisante des données en entrée → buffer overflow
    - À distance + sans privilèges spécifiques = vol de jetons de session
    - Affecte les appliances Citrix ADC et Citrix Gateway
      - Configurées en tant que fournisseur d'identité SAML !
- Patchez ! Versions affectées :
  - Version 13.1 de Citrix NetScaler ADC et NetScaler Gateway
  - Version 13.1-FIPS et 13.1-NDcPP de NetScaler ADC

https://www.it-connect.fr/cve-2026-3055-appliquez-ce-patch-citrix-avant-quil-ne-soit-trop-tard/

Failles / Bulletins / Advisories
Navigateur (principales failles)

Partenariat Claude Opus 4.6 + Firefox

- Découverte de 22 failles en 2 semaines
  - 14 élevées, 7 modérées et 1 faible
  - Première faille type « Use after free » trouvée en 20 min
- 90 bugs ont aussi été identifiés



Source : Anthropic

https://www.it-connect.fr/firefox-148-22-failles-de-securite-corrigees-grace-a-ia-claude-opus-4-6/

Failles / Bulletins / Advisories
Navigateur (principales failles)

34 vulnérabilités corrigées en moins d'une semaine ! #Chrome

- En 2 phases :
  - 26 corrigées le 18 mars
  - 8 corrigées le 23 mars
- Aucune vulnérabilité exploitée dans la nature
- Tout de même 3 failles critiques :
  - [**CVE-2026-4439**] Type « Out of bounds access », WebGL
  - [**CVE-2026-4440**] Type « Out of bounds read », WebGL
  - [**CVE-2026-4441**] Type « Use after free », composant Base
- Patchez !
  - Windows & MacOS : 146.0.7680.164/165
  - Linux : 146.0.7680.164

https://www.it-connect.fr/google-chrome-34-vulnerabilites-corrigees-en-quelques-jours/

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

Gemini en open bar

- Possible d'utiliser les clés de projet pour appeler l'API Gemini
  - Vulnérabilité car permissions au niveau du projet, pas au niveau de la clé
- Clés API légitimes, comme pour utiliser Google Maps
- Google a classé cela comme une élévation de privilèges
  - Bloquer les clés utilisées pour accéder à son API de façon illégitime

https://www.it-connect.fr/ia-les-cles-api-google-publiques-donnent-acces-a-gemini/

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

Le bloc-notes de Microsoft mis à jour

- Possible de lancer des programmes malveillants en cliquant sur un lien formaté en Markdown
  - Lien pointant vers un exécutable interne au lieu d'un lien hypertexte
- PoC disponible → https://github.com/BTtea/CVE-2026-20841-PoC
- Mise en place d'un garde fou de Microsoft pour analyser les liens

https://www.it-connect.fr/une-faille-dans-bloc-notes-permet-de-lancer-un-executable-sur-windows-11-avec-un-lien-markdown/

CVE-2026-20841

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

Faille dans Windows Admin Center

CVE-2026-26119

- Authentification malveillante pouvant entraîner une privesc sur le réseau
  - Usurpation d'un compte admin = compromission du domaine
  - « Dans certaines conditions, ce problème pourrait permettre la compromission complète d'un domaine à partir d'un utilisateur standard. »
- Faille sécurité dans la version 2511 de WAV
  - Version publiée en décembre 2025

https://thehackernews.com/2026/02/microsoft-patches-cve-2026-26119.html

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

Echapper de son Docker


CVE-2026-34040

- Faille découverte dans Docker Engine
  - Permet de contourner le plugin de gestion des autorisations (AuthZ)
  - Liée à la **CVE-2024-41110** qui n'avait pas correctement été patchée
- Via une requête API
  - Amener le démon à transmettre la requête à un plugin d'autorisation sans son body
    - Le plugin pourrait accepter la requête alors qu'il l'aurait autre refusée avec son body transmis
- Patch de l'époque :
  - Check de Content-Length (pour le body) > 0
  - Problème : qu'est-ce qui se passe quand sa valeur est trop grande ?
- But de l'exploitation :
  - Créer un conteneur privilégié avec un accès root à l'hôte Docker
- Passez sur Docker Engine 29.3.1 !
  - Concernant la version Docker Desktop, passez sur sa version 4.66.1

https://www.it-connect.fr/docker-la-faille-cve-2026-34040-permet-dobtenir-un-acces-root-sur-lhote/

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

Faille dans FortiClient EMS

CVE-2026-21643

- Remontée comme étant exploitée par Defused
- Faille de type « SQL Injection »
  - Exploitable à distance et sans authentification requise
  - Exécution de cote arbitraire ou de commande sur la machine possible
- Version affectée : 7.4.4
- 2.000 instances FortiClient EMS exposées sur Internet 😥

https://www.bleepingcomputer.com/news/security/critical-fortinet-forticlient-ems-flaw-now-exploited-in-attacks/

Failles / Bulletins / Advisories
Smartphone (principales failles)

Apple : 1er correctif de sécurité déployé via Background Security Improvements

- Fonctionnalité permettant de patcher sans avoir besoin de redémarrer l'appareil
- Vulnérabilité corrigée ?
  - Type « cross-origin » au sein de l'API de navigation de WebKit
    - Et donc de contourner la politique Same Origin (du navigateur)
- Appareils concernés :
  - iOS 26.3.1
  - iPadOS 26.3.1
  - macOS 26.3.1 et 26.3.2

https://www.it-connect.fr/apple-a-corrige-une-faille-sur-ios-et-macos-et-cest-invisible-grace-a-cette-nouveaute/

CVE-2026-20643

Piratages, Malwares, spam, fraudes et DDoS

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Le FBI hacké

- Plus exactement la boîte mail du patron du FBI, sa boîte mail personnelle
  - Attaque revendiquée par le groupe de pirate Handala
  - Données récupérées datant de 2010 à 2019
  - Pas de données professionnelles heureusement

https://www.it-connect.fr/le-patron-du-fbi-sest-fait-hacker-sa-boite-mail-personnelle-par-le-groupe-handala/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

80.000 PC impactés mais pas de malware

- Suppression des données sur le parc de Stryker
  - Postes de travail, serveurs et appareils mobiles corrompus
- Pas de malware ici…
- Compromission d'un compte admin sur l'environnement 365
  - Création d'un nouvel admin Global
  - Exécution de « `Wipe` » pour supprimer les données
- L'attaquant indique avoir volé 50 To de données
  - Aucune preuve d'exfiltration trouvée

https://www.it-connect.fr/comment-les-pirates-ont-efface-80-000-pc-chez-stryker-sans-le-moindre-malware/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Le ver de 23 minutes de Wikipédia

- Bout de code hébergé sur la version russe de Wikipédia, présent sur les serveurs depuis mars 2024. Script déclenché le 5 mars 2026
  - « Patient zéro » : compte appartenant à un employé de la Wikimedia Foundation
- Ciblage de 2 types de fichiers :
  - « `User:<username>/common.js` »
  - « `MediaWiki:Common.js` »
- Objectif : Vandaliser le contenu
  - Appel d'une fonction Random
- Bilan : 3 996 pages vandalisées et 85 comptes utilisateurs altérée par le ver

https://www.it-connect.fr/pendant-23-minutes-ce-ver-javascript-a-seme-la-pagaille-sur-wikipedia/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Trivy compromis (x2) → attaque supply chain majeure

- Compromis 2 fois en 3 semaines
  - Fin février 2026 : compromission initiale (token GitHub volé via CI/CD)
    - Merci HackerBot Claw (bot IA) #TeamPCP
  - 19 mars : publication version piégée v0.69.4
    - Avec un infostealer 🎁
  - 20–21 mars : suppression + rollback (v0.69.3)
  - 22–23 : nouvelle vague → images Docker compromises (0.69.5 / 0.69.6)
- Publications effectuées via plusieurs canaux :
  - GitHub Releases, Homebrew et Docker Hub
  - + utilisation de comptes légitimes = supply chain « trusted channel »

https://www.bleepingcomputer.com/news/security/trivy-supply-chain-attack-spreads-to-docker-github-repos/

Piratages, Malwares, spam, fraudes et DDoS
Piratage

Piratage de LiteLLM (paquet Python)

- Encore un coup de la TeamPCP !
- 2 versions malveillantes publiées le 24 mars : 1.82.7 et 1.82.8
  - Avec une charge malveillante 🎁
- Attaque en 3 étapes :
  1. Récupération des identifiants :
     - Clés SSH, jetons cloud, secrets Kubernetes, portefeuilles cryptographiques, fichiers système, .env, etc.
  2. Propagation vers d'autres ressources
     - Par l'intermédiaire des clusters Kubernetes via le déploiement de pods privilégiés sur chaque nœud
  3. Installation d'une porte dérobée persistante via systemd
- Paquet téléchargé 3 millions de fois par jour…

https://www.it-connect.fr/piratage-de-litellm-des-millions-dutilisateurs-python-sous-la-menace-de-teampcp/

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

Des données et du poulet en ligne

- Vol de données chez KFC via un accès illégitime
  - Aucune information sur la taille des données volés
  - Type d'information volées :
    - Nom, prénom, e-mail, numéro de téléphone et numéro de fidélité Colonel Club
- Plainte contre X déposée auprès du procureur de la République du tribunal judiciaire de Nanterre
- Mail de communication envoyé aux concernés

https://www.it-connect.fr/fuite-de-donnees-chez-kfc-france-les-clients-du-programme-fidelite-touches/

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

12 Go de données volées chez Aura

- Entreprise américaine dans la protection d'identité
- Mise en ligne après que la demande de rançon ait échoué
  - Noms complets, e-mail, adresses postales, numéros de téléphone, adresses IP et journaux de commentaires du service client
- Présence aussi de données de personnes NON CLIENTES
  - De nombreuses données proviendraient d'une entreprise rachetée par Aura en 2021

https://www.it-connect.fr/le-specialiste-de-la-protection-identite-aura-pirate-900-000-contacts-dans-la-nature/

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

Supply Chain chez ManoMano

- 38M d'utilisateurs impactés
  - Accès illégitime détecté sur les serveurs par un prestataire
  - Compromission d'un compte utilisateur d'un centre de support basé à Tunis
  - Extraction des données en janvier 2026
- Données impactées :
  - Nom complet, e-mail, numéro de téléphone et communications et échanges avec le service client (tickets de support, requêtes, etc.)

https://www.it-connect.fr/manomano-38-millions-de-clients-impactes-par-une-fuite-de-donnees/

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

Accident le 1er avril 🐟

- Fuite du code source de Claude Code
  - Mise en ligne du fichier `cli.js.map`
  - Correspond à la version 2.1.88 sur le registre NPM
  - La fuite représente 1.900 fichiers et 512.000 lignes de code
- Claude décide de traquer ceux qui partagent le code

https://www.it-connect.fr/anthropic-le-code-source-de-loutil-claude-code-fuite-sur-le-web/

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

Les étudiants à risque

- Exfiltration des données du site mesrdv.etudiant.gouv.fr
- 774.000 étudiants impactés
  - 80% des étudiants uniquement concernés sur des données habituelles
  - Données plus sensibles pour les 20% restants
    - Copie de document délicat : carte d'identité, passeport…
- Groupe de pirate identifié : DumpSec

https://www.it-connect.fr/piratage-du-crous-les-donnees-de-774-000-etudiants-dans-la-nature-mars-2026/

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

Et les enseignants aussi victimes

- Compromission d'identifiants d'un compte du site COMPAS
- Vol des données de 243.000 enseignants
  - Les noms et prénoms, dates de naissance, numéros d'identification et de téléphone, adresses postales et périodes d'absences
- Risque de campagnes de phishing ciblées

https://www.it-connect.fr/piratage-education-nationale-le-portail-compas-pirate-243-000-enseignants-touches/

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

Footing fatal sur le porte-avion Charles-de-Gaulle #StravaLeaks

- Coupable : un militaire faisant son footing avec une montre connectée
  - Reliée à un compte Strava public
- Conséquence : possibilité de suivre quasiment en temps réel la localisation du porte-avion
  - Pendant 35 minutes ! (7 km d'Arthur)

https://www.lemonde.fr/international/article/2026/03/19/stravaleaks-le-porte-avions-charles-de-gaulle-localise-en-temps-reel-par-le-monde-grace-a-l-application-de-sport_6672445_3210.html

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

Incident Cegedim : fuite de données impactant entre 11 et 15 millions de français

- Suite à une intrusion sur MonLogicielMedical.com
  - Solution développée par Cegedim Santé (filiale du groupe Cegedim)
  - Solution utilisée par 3.800 médecins en France dont 1.500 concernés
- Contient les informations habituelles :
  - Nom, prénom, sexe, adresse postale, adresse e-mail et date de naissance
- MAIS aussi un champs texte libre…
  - … où les médecins inscrivent des observations brutes pour le suivi de leurs patients
  - Extraits venant de France 2 :
    - « porteuse sida !!! !!!! »
    - « serait homosexuelle d'après sa mère »
    - « mère musulmane voilée »
    - « catholique non pratiquante car ses 2 frères sont suicidés »
    - « Fils en prison »
- Parmi les victimes : des personnalités politiques !
  - Dont de potentiels candidats à l'élection présidentielle et de hauts fonctionnaires

https://www.it-connect.fr/incident-cegedim-cette-fuite-de-donnees-medicales-menace-lintimite-de-millions-de-francais/

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

Fuite de données chez Alinto exposant du trafic email

- Base Elasticsearch non sécurisée accessible publiquement
  - = 40 millions de logs SMTP exposés
  - Corrigé rapidement après divulgation (mais fenêtre inconnue)
- Données exposées ?
  - Adresses email (expéditeur / destinataire)
  - Horodatages + IP relais
  - Données de localisation
- De grandes entreprises concernées impactées comme L'Oréal, Renault, DHL…
- Au mois 14.000 adresses gouvernementales françaises exposées
- Les métadonnées = renseignement stratégique
  - Cartographie des relations (qui parle à qui)
  - Analyse des habitudes (quand, fréquence)
  - Identification des personnes clés

https://cybernews.com/security/alinto-email-data-leak-exposes-traffic/

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

Fin de YggTorrent

- Arrêt brutal associé à la publication d'une archive de 11 Go sur le site yggleak[.]top
  - Auteur du piratage : Grolum
- Il dénonce les pratiques du site :
  - Recettes de la plateforme YggTorrent : 10 millions d'euros pour 2024-2025
    - « Alors que vos équipes de modérateurs bossent bénévolement pour faire tourner le site, vous continuez d'amasser une véritable fortune sur leur dos. Francisco depuis le Maroc et Vladimir depuis la France, vous avez exploité la naïveté de personnes qui croyaient en un projet de partage libre, désintéressé et communautaire. »
  - Interception de 54.776 cartes bancaires
  - Scan de cryptomonnaies
  - Moitié des mots de passe stockés en MD5
- Archive ZIP contenant :
  - Code source, documents, bases de données, identifiants et autres nombreuses informations

https://www.it-connect.fr/fin-de-yggtorrent-un-pirate-detruit-le-site-et-revele-les-pratiques-mafieuses-de-ses-admins/

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

Accès au fichier FICOBA

- Victime de cette fuite ? La Direction Générale des Finances publiques (DGFiP)
- Fichier FICOBA ?
  - Base de données critique recensant l'intégralité des comptes ouverts dans les établissements bancaires français
  - Informations sensibles de près de 1.2 millions de personnes dérobées depuis janvier 2026
    - Identité complète du titulaire
    - Coordonnées postales
    - Coordonnées bancaires (RIB / IBAN)
    - Identifiant fiscal de l'usager (dans certains cas)
- Source de l’intrusion venant de la compromission du compte d’un fonctionnaire
- Risque élevé d'attaque par ingénierie sociale et par hameçonnage !

https://www.impots.gouv.fr/actualite/acces-illegitimes-au-fichier-national-des-comptes-bancaires-ficoba

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

Fuite de données chez la CFDT qui impacte ses adhérents

- Victime d'une attaque informatique
  - Impliquant le téléchargement des données personnelles d'adhérents :
    - Le couple prénom et nom
    - Les coordonnées complètes de contact
    - La date d'adhésion à la CFDT
    - Le syndicat d'affiliation précis
- 1.4 millions de membres affectés
  - Informations sur les membres actifs ET sur d'anciens affiliés
    - « En tant qu'ex-adhérent.e, vos données ont pu être impactées : en effet, et conformément aux dispositions légales et réglementaires, nous conservons les données de nos ex-adhérent.es pour une durée de 4 ans à partir de la clôture de l'exercice après leur départ de la CFDT, et pendant 10 ans en ce qui concerne les documents comptables (par exemple les pièces justificatives de remboursement de frais). »

https://next.ink/brief_article/la-cfdt-confirme-un-vol-de-donnees-qui-concerne-aussi-les-ex-adherents/

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

Piratage de la Commission européenne

- Revendiqué par ShinyHunters
- Intrusion effectuée sur le portail officiel : Europa.eu
  - Grâce à un accès malveillant à un compte AWS utilisée par la Comission
- 350 Go de données volées :
  - Bases de données
  - Documents confidentiels
  - Contrats
- La Commission européenne est restée muette à ce sujet

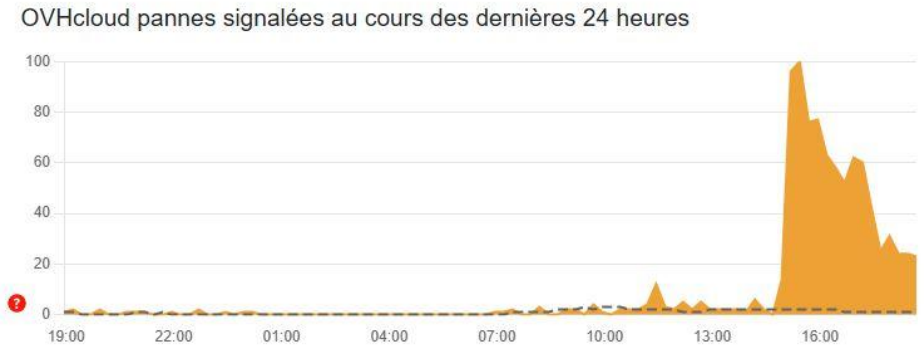
https://www.bleepingcomputer.com/news/security/european-commission-confirms-data-breach-after-europaeu-hack/

Piratages, Malwares, spam, fraudes et DDoS
Panne

Panne OVH

- A eu lieu le lundi 23 février
  - À partir de 15h11
- Plusieurs sites français inaccessibles
  - Comme Gameblog, Clubic et OpenClassrooms
- Cause : problème électrique dû à une défaillance matérielle
  - Dans une partie du data center de Gravelines

https://www.lesnumeriques.com/societe-numerique/une-panne-ovh-a-rendu-plusieurs-sites-francais-inaccessibles-n251889.html



Piratages, Malwares, spam, fraudes et DDoS
Publication

ANSSI : mise à jour de la politique Open Source

- S’intitule autour de 4 axes
  - Publier des logiciels sous licences libres
  - Contribuer à des projets open source existants
  - Renforcer et structurer l’écosystème open source
  - Utiliser des solutions open source au sein de l’ANSSI
- Finance des audits de sécurité de logiciels open source
  - Objectif : sécuriser des composants très utilisés

https://cyber.gouv.fr/enjeux-technologiques/open-source/

Piratages, Malwares, spam, fraudes et DDoS
Publication

ANSSI : panorama de la cybersécurité 2025

- Bilan de l'année
  - Présente un nombre constant du volume d'attaque…
  - Mais des impacts plus graves et plus stratégiques
- + 1.366 incidents traités par l'ANSSI
- Moins d'attaque de type ransomware
  - Mais des attaques à réaction (vol et exploitation des données)
- Présente des menaces plus difficiles à détecter et restreindre
  - La vente de malware en ligne
  - Le partage d'outils entre attaquants
  - Des chaînes d'attaque de + en + sophistiquées

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf

Piratages, Malwares, spam, fraudes et DDoS
Publication

La chute du TTE

- Le délai entre divulgation d'une vulnérabilité et exploitation (TTE) s'est effondré
  - 2018 : ~ 771 jours pour exploiter une vulnérabilité
  - 2021 : 84 jours
  - 2023 : 6 jours
  - 2024 : 4 heures
  - 2025 : ~ 0 jour (avant disclosure)
- ~30% des CVES exploitées en < 24h
  - La fenêtre de réaction a disparu
- Avant : modèle « patcher à temps » → Maintenant : l'attaque précède la défense
- L'IA favorise intrinsèquement l'offense :
  - découvre des vulnérabilités
  - génère des exploits
  - automatise les attaques

https://zerodayclock.com/

Business et Politique

Droit / Juridique / Politique
Monde

Freedom[.]gov, le VPN d'état américain

- Destiné au grand public et se voit comme un outil d'anti-censure
  - Censé permettre aux utilisateurs du monde de contourner les mesures de blocage sur des sites et des contenus du pays
- S'oriente directement pour aller à l'encontre des autres états (blocage porngographique pour les mineures en France)
- Promesse de l'état de ne pas pister les utilisateurs… 😳

https://www.numerama.com/politique/2183583-les-etats-unis-preparent-un-vpn-detat-pour-inciter-les-europeens-a-contourner-les-lois.html

Conférences

Conférences

Passée(s)

- JSSI, 10 mars à Paris
  - ○ Sujet : << La Supply Chain, maillon faible de la Cyber >>
- CoRIIN, 31 mars à Lille
  - ○ En parallèle du FIC
- FIC, 31 mars au 2 avril à Lille

À venir

- sambaXP, 20 au 21 avril en ligne
- Botconf, 15 au 17 avril à Reims
- SSTIC, 3 au 5 juin à Rennes
- LeHACK, 26 au 28 juin à Paris
- Pass the SALT, 30 juin au 2 juillet à Lille

Divers / Trolls velus

Divers / Trolls velus

ChatGPT VS avocats

- En 2021, rachat du studio Unknown Worlds Entertainment par l'éditeur Krafton pour 500M$
  - Condition dans le contrat : si prochain jeu atteint un objectif → + 250M$
- Ne voulant pas payer, l'éditeur a :
  - Licencié les fondateurs du studio
  - Repris le contrôle du projet
  - Influencé l'opinion publique
- Sous les conseils « avisés » de ChatGPT au détriment de ceux des avocats qui prévenait du risque d'une action en justice
- Perte du procés pour l'éditeur, réinsertion des dirigeants et revue des contrats

https://www.science-et-vie.com/technos-et-futur/un-pdg-remplace-ses-avocats-par-chatgpt-et-perd-un-proces-a-250-millions-231292.html

Divers / Trolls velus

Don’t go to the Police

- Documentaire réalisé par Orange
- Retrace la traque de 2023 contre LockBit suite à l’attaque contre Coaxis
- 18 interviews avec différents acteurs : dirigeants coaxis, expert cybersécurité, agents du FBI…

https://dontgotothepolice.orangecyberdefense.com/fr

Divers / Trolls velus

iOS 26 certifié par l'OTAN

- iPhone et iPad sous iOS 26 ont été homolgué « NATO Restricted »
  - 1er niveau, permettant d'héberger des données confidentielles
- Audit de sécurité réalisé par la BSI
  - Lien du rapport disponible
  - Analyse de la configuration spécifique « indigo »
    - Elle correspond à un accès sécurisé aux contacts, aux calendriers et aux e-mails
    - Sécurité intégré à l'équipement sous la supervision d'un MDM

https://www.it-connect.fr/ios-26-iphone-certifie-par-otan-pour-traiter-les-donnees-classifiees/

Divers / Trolls velus

Réduction de la durée de vie des certificats SSL/TLS

- Durée de validité maximale des certificats ?
  - Avant le 15 mars 2026 : = 398 jours (environ 13 mois)
  - À partir du 15 mars 2026 = 200 jours (environ 6.5 mois)
  - À partir du 15 mars 2027 = 100 jours (environ 3 mois)
  - À partir du 15 mars 2029 = 47 jours (environ 1.5 mois)
- Important !
  - Les certificats émis avant chaque date limite resteront valides jusqu'à leur date d'expiration initiale
- Objectif principal :
  - Renforcer la sécurité et d'améliorer la réactivité face aux incidents
    - Et palier aux systèmes de révocation traditionnels (CRL, OCSP) souvent lents ou peu fiables
- Merci au CA/Browser Forum

https://www.chambersign.fr/actualites/reduction-duree-de-vie-certificats-ssl-tls-2026/

Divers / Trolls velus

La fin du chiffrement de bout en bout (E2EE) sur Instagram

- En place dès le 8 mai 2026 !
- Raison principale évoqué :
  - Fonctionnalité peu utilisée par les utilisateurs #Rétropédalage
    - Donc ce n'était pas activé par défaut…
  - La fonction avait été introduite en 2023
- Une autre raison ?
  - Une concession stratégique face aux autorités ?
  - Plutôt qu'à un choix justifié vis-à-vis de l'expérience des utilisateurs ?

https://www.it-connect.fr/fin-du-chiffrement-de-bout-en-bout-sur-instagram-des-le-8-mai-2026/

Divers / Trolls velus

Rappel : Windows – Expiration des certificats Secure Boot & mises à jour CA

- cf. https://www.ossir.org/paris/supports/2025/2025-10-14/2025-10-14.pdf (page 38)
  - Les premiers certificats expirent en juin 2026 !
- Systèmes éligibles à la réception automatique des nouveaux certificats :
  - Windows 11 (toutes les versions)
  - Windows 10 version 22H2 et ultérieures (y compris 21H2 LTSC)
  - Windows Server 2022 et 2025
  - Windows Server 2016 et 2019
  - Windows Server 2012 / 2012 R2 (uniquement celles où le programme ESU est actif)
- Les machines où Secure Boot est désactivé dans le BIOS ne recevront pas ces mises à jour !
- Ne pas mettre à jour ces certificats =
  - Perdre la capacité d'appliquer les mises à jour de sécurité relatives au Secure Boot après juin 2026
  - Devenir incapables de valider les logiciels tiers signés avec les nouveaux certificats après juin 2026
  - Cesser de recevoir les correctifs de sécurité pour Windows Boot Manager après octobre 2026
- Check HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing\UEFICA2023Status + déployer par GPO ou par Microsoft Intune !

https://www.it-connect.fr/fin-du-chiffrement-de-bout-en-bout-sur-instagram-des-le-8-mai-2026/

Divers / Trolls velus

BrowserGate : scan silencieux effectué par LinkedIn ?

- Publié par Fairlinked e.V. (une association d'utilisateurs commerciaux de LinkedIn)
- Un script JavaScript injecté lors des sessions de navigation sur LinkedIn ?
  - Objectif : détecter la présence des extensions de navigateur en effectuant une recherche sur des identifiants d'extensions connus
    - ~ 6 236 extensions différentes sur les navigateurs basés sur Chromium
- Une empreinte numérique de l'appareil de l'utilisateur est également créée :
  - Le nombre de cœurs du processeur
  - La mémoire vive (RAM) disponible
  - La résolution de l'écran
  - Le fuseau horaire et la langue du système
  - L'état de la batterie et les paramètres audio
- Réponse de LinkedIn : « Nous utilisons ces données pour identifier les extensions qui enfreignent nos conditions d'utilisation, pour adapter et améliorer nos mesures de protection techniques, et pour comprendre pourquoi le compte d'un membre pourrait récupérer un volume excessif de données appartenant à d'autres membres, ce qui, à grande échelle, nuit à la stabilité du site. »

https://www.bleepingcomputer.com/news/security/linkedin-secretly-scans-for-6-000-plus-chrome-extensions-collects-data/

FIN

Prochaine réunion ?

- RDV le **mardi 12 mai 2026**

Accéder aux différents supports ?

Replays

Slides

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

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