CPAM Ardèche / Greta Ardèche-Drôme

Procédure veille technologique

TP

Collet Valentin
BTS SIO-SISR / Session 2026

SOMMAIRE

Cahier des charges

Descriptifs de l'existant

Pour la mise en place de la veille, les ressources suivantes sont disponibles dès le début de la mission :

Postes de travail : PC sous Windows 10 Pro, 8 Go RAM, navigateur web (Firefox / Chrome), accès internet illimité.

Compte Feedly :

Compte gratuit à créer sur feedly.com pour agréger les flux RSS de toutes les sources officielles de cybersécurité (CERT-FR, MSRC, Debian DSA, ANSSI, NVD NIST, Krebs on Security). La version gratuite permet jusqu'à 100 sources et 3 collections thématiques, ce qui est suffisant pour cette veille. L'accès se fait via navigateur web (Firefox ou Chrome) sur les postes du GRETA, ou via l'application mobile Feedly (iOS / Android).

Accès aux sources :

Accès libre aux sites officiels CERT-FR (cert.ssi.gouv.fr), MSRC (msrc.microsoft.com), Debian Security (security.debian.org), ANSSI (ssi.gouv.fr) et NVD NIST (nvd.nist.gov).

Durée de la mission :

6 mois, de septembre 2025 à février 2026, avec une session de veille hebdomadaire minimum d'une heure sur les nouvelles publications.

Besoins

Dans le cadre du BTS SIO option SISR, il est demandé de mettre en place une veille technologique portant sur la cybersécurité des systèmes d'exploitation Microsoft (Windows 10/11, Windows Server) et des distributions Debian Linux. Cette veille doit être conduite sur une durée de six mois, de septembre 2025 à février 2026, à raison d'une session de lecture hebdomadaire minimum.

La veille doit permettre d'assurer un suivi rigoureux des vulnérabilités publiées (CVE), des correctifs de sécurité (notamment les Patch Tuesday Microsoft et les Debian Security Advisories), ainsi que des menaces et incidents notables susceptibles d'affecter les environnements supervisés. Chaque mois, deux articles ou bulletins représentatifs doivent être sélectionnés, analysés et synthétisés dans un rapport mensuel destiné à démontrer la maîtrise des sources et la capacité à évaluer l'impact d'une vulnérabilité sur un système d'information.

L'outil de veille retenu doit être accessible gratuitement, simple à prendre en main et compatible avec les ressources disponibles en salle TP. Il doit permettre d'agréger des sources hétérogènes (flux RSS, bulletins officiels, blogs spécialisés) dans une interface

centralisée, afin de rationaliser le temps consacré à la lecture et d'éviter la dispersion entre de multiples sites et plateformes.

Contraintes

Temps :

La veille est réalisée en dehors des cours, idéalement avec 2h allouée à celle-ci par semaine.

Sources :

L'information retenue doit provenir de sources vérifiées et reconnues : CERT-FR, MSRC (Microsoft), Debian Security Advisories, ANSSI, NVD NIST. Les blogs anonymes ou les forums non modérés ne sont pas des sources valides.

Budget :

Aucun budget n'est alloué. Tous les outils utilisés (Feedly version gratuite, flux RSS publics, réseaux sociaux) doivent être accessibles sans frais. La version gratuite de Feedly permet jusqu'à 100 sources et 3 collections, ce qui est suffisant pour cette veille. Les fonctionnalités avancées de Feedly Pro (filtrage automatique par mots-clés, intégrations tierces) ne sont pas nécessaires dans le cadre de ce TP.

Couverture obligatoire :

La veille doit couvrir impérativement les deux environnements ciblés : Microsoft / Windows (CVE, Patch Tuesday, bulletins MSRC) et Debian Linux (DSA - Debian Security Advisories, correctifs de paquets critiques).

Maîtrise de l'anglais technique :

La majorité des sources de référence (MSRC, NVD NIST, Krebs on Security, BleepingComputer) publient en anglais. La lecture et la compréhension des bulletins techniques en anglais est indispensable.

Fiabilité des sources face au volume d'informations :

Le volume d'informations disponibles en matière de cybersécurité est considérable et en constante augmentation. Entre les bulletins officiels, les blogs spécialisés, les réseaux sociaux et les agrégateurs d'actualités, il est difficile de distinguer rapidement une information fiable et vérifiée d'une rumeur, d'une analyse incorrecte ou d'un contenu publicitaire déguisé. Cette contrainte impose de s'appuyer en priorité sur des sources institutionnelles reconnues (CERT-FR, ANSSI, MSRC, Debian Security Team, NVD NIST) et de croiser les informations avant toute diffusion ou prise de décision, même lorsque cela ralentit le processus de veille.

Ressources

Les ressources mobilisées pour la veille sont les suivantes :

Réseaux sociaux (LinkedIn, X/Twitter, Reddit r/netsec) :

Comptes gratuits permettant de suivre en temps réel les annonces des chercheurs, éditeurs (comptes @MsftSecIntel, @certfr) et de la communauté cybersécurité. Utilisés en complément des flux RSS pour les informations urgentes et les discussions de la communauté.

CVE (Common Vulnerabilities and Exposures) :

Une CVE (Common Vulnerabilities and Exposures) est un identifiant standardisé attribué à une vulnérabilité de sécurité connue dans un logiciel ou un système. Chaque CVE est référencée dans la base de données nationale américaine NVD (National Vulnerability Database, nvd.nist.gov) et se présente sous la forme CVE-ANNÉE-NUMÉRO (par exemple : CVE-2025-54918). Elle est accompagnée d'un score de criticité CVSS (Common Vulnerability Scoring System) compris entre 0 et 10, permettant d'évaluer rapidement la gravité de la faille : Critique (9.0–10.0), Élevée (7.0–8.9), Moyenne (4.0–6.9), Faible (0.1–3.9). Suivre les CVE publiées est au cœur de la veille en cybersécurité, car elles constituent l'indicateur principal de l'exposition d'un système à des risques connus et documentés.

Remarque : Le flux Security Update Guide (api.msrc.microsoft.com/update-guide/rss) publie en temps réel chaque CVE ajoutée par Microsoft, y compris les bulletins mensuels Patch Tuesday (second mardi du mois) et les alertes hors-cycle (OOB). C'est la source officielle la plus complète pour suivre toutes les vulnérabilités Microsoft. Krebs on Security (krebsonsecurity.com/feed/) complète ce flux avec des résumés contextualisés des Patch Tuesday, accessibles en français-compatible et très utiles pour prioriser les correctifs critiques.

Feedly (agrégateur RSS) :

Plateforme web gratuite (feedly.com) permettant de centraliser l'ensemble des flux RSS dans une interface unique. Les flux sont organisés en trois Collections thématiques : « Windows / Microsoft » (MSRC, Krebs on Security), « Debian / Linux » (DSA Debian, LWN.net), « Cybersécurité Générale » (CERT-FR, ANSSI, NVD NIST, Krebs on Security). Feedly propose une application mobile iOS/Android pour consulter les flux en mobilité, ainsi qu'un système de Boards (tableaux de bord) pour sauvegarder et classer les articles importants. L'inscription est possible via un compte Google ou une adresse e-mail. La version gratuite est suffisante pour l'ensemble de cette veille.

Matériel informatique :

Poste de travail sous Windows 11 avec navigateur web pour la consultation de feedly (possible aussi sur smartphone) et des sources.

AI :

Je me suis aidé de Claude.ai afin de trier les CVE avec une criticité élevé, puis j'ai lu les articles ainsi trier, ceci m'a aidé à m'y retrouver dans la masse d'information que ma veille a remonté, en priorisant les CVE les plus critiques j'ai pu orienté ma veille sur les failles les plus importantes.

Analyse

Descriptif des solutions

Réseaux sociaux (LinkedIn, X/Twitter, Reddit) :

Les réseaux sociaux constituent une source de veille en temps réel. Des professionnels de la sécurité informatique, des chercheurs et des organismes officiels (comme le CERT-FR ou Microsoft) publient régulièrement des alertes et des analyses. LinkedIn permet de suivre des experts en sécurité et des entreprises spécialisées (Kaspersky, CrowdStrike, etc.). Reddit via les communautés r/netsec, r/debian propose des discussions techniques sur les vulnérabilités et les correctifs. L'inconvénient majeur reste la difficulté à filtrer l'information de qualité parmi le volume de publications.

Flux RSS :

Les flux RSS (Really Simple Syndication) permettent de s'abonner directement aux publications de sources officielles sans dépendre d'algorithmes. Ils offrent une grande fiabilité : les organismes comme le CERT-FR (cert.ssi.gouv.fr), l'ANSSI, le MSRC (Microsoft Security Response Center, msrc.microsoft.com) et les advisories Debian Security (security.debian.org) proposent tous des flux RSS. Chaque nouvelle vulnérabilité ou correctif publié apparaît automatiquement dans le lecteur.

Feedly :

Feedly est une plateforme web de gestion de flux RSS disponible gratuitement. Elle permet d'agréger les publications de multiples sources dans une interface unique, organisée en Collections thématiques. Contrairement à la consultation directe de chaque site, Feedly centralise les nouvelles publications et permet une lecture efficace sans avoir à visiter chaque source individuellement. La version gratuite propose jusqu'à 100 sources et 3 collections, un système de sauvegarde d'articles (Saved / Boards) pour archiver les publications importantes, une application mobile synchronisée, et des

notifications e-mail paramétrables. Feedly est utilisé par des milliers de professionnels de la cybersécurité pour leur veille technologique quotidienne.

Comparaison des solutions :

Critères	Réseaux sociaux	Flux RSS	Feedly
Fiabilité des sources	Moyenne (non filtrée)	Élevée (sources officielles)	Élevée (agrège sources fiables)
Temps réel	Oui	Variable (délai de publication)	Oui (mise à jour horaire)
Facilité de gestion	Difficile (dispersion)	Complexe sans outil	Simple (interface centralisée)
Classement/filtrage	Limité	Limité sans lecteur	Basique (Boards manuels, sans auto)
Accès mobile	Oui	Non natif	Oui (application dédiée)
Couverture Microsoft & Debian	Partielle (selon comptes suivis)	Complète (sources officielles)	Complète (flux configurés)
Recherche & historique	Limité (algorithmes sociaux)	Non (sans outil dédié)	Oui (recherche intégrée, archive)
Coût	Gratuit	Gratuit	Gratuit (version de base)

Choix d'une solution

La solution retenue est la combinaison des flux RSS agrégés via Feedly. Cette approche offre le meilleur rapport entre fiabilité des sources, facilité de gestion, couverture complète des environnements Microsoft et Debian, et gratuité de l'outil. Feedly centralise dans une interface unique toutes les sources officielles sélectionnées, organise les flux en trois Collections thématiques, et permet de sauvegarder les articles importants dans des Boards dédiés (Critique, Important, Veille mensuelle). L'accès est possible depuis les postes du GRETA (navigateur web) et en mobilité via l'application Feedly.

Les réseaux sociaux seront utilisés en complément pour suivre les annonces en temps réel de certains acteurs clés (compte Twitter/X du CERT-FR, compte LinkedIn de l'ANSSI), mais ne seront pas la source principale en raison du manque de fiabilité et de la difficulté de filtrage.

Les sources RSS sélectionnées seront :

- CERT-FR (cert.ssi.gouv.fr/feed/) : alertes de sécurité du centre gouvernemental français
- MSRC – Security Update Guide (flux CVE officiel Patch Tuesday) : https://api.msrc.microsoft.com/update-guide/rss
- Krebs on Security (krebsonsecurity.com/feed/) : résumés Patch Tuesday et analyses CVE Microsoft
- Debian Security Advisories (security.debian.org) : CVE et correctifs spécifiques Debian
- NVD NIST (nvd.nist.gov) : base de données nationale des vulnérabilités américaine pour les CVE
- Krebs on Security (krebsonsecurity.com/feed/) : blog de référence en cybersécurité

Phasage de l'intervention

1) Création du compte Feedly sur feedly.com et configuration initiale de l'interface

2) Création des trois Collections thématiques : « Windows / Microsoft », « Debian / Linux », « Cybersécurité Générale »

3) Ajout des flux RSS des sources officielles Microsoft (MSRC, Krebs on Security) dans la collection Windows / Microsoft

4) Ajout des flux RSS des sources Debian (Security Advisories DSA, LWN.net) dans la collection Debian / Linux

5) Ajout des flux RSS des sources généralistes cybersécurité (CERT-FR, ANSSI, NVD NIST, Krebs on Security) dans la collection Cybersécurité Générale

6) Création des Boards de classement (« Critique – À traiter », « Important – À planifier », « Veille mensuelle »

8) Suivi régulier hebdomadaire des publications (minimum 1 session de lecture par semaine, sauvegarde des articles importants dans les Boards)

Test : Vérification que les flux RSS sont bien actifs, que de nouveaux articles apparaissent dans chaque Collection, et que la sauvegarde dans les Boards fonctionne correctement.

Mise en place

Cette section détaille l'ensemble des opérations à réaliser pour mettre en place la veille technologique sur Feedly, depuis la création du compte jusqu'au protocole de lecture hebdomadaire. Feedly est un agrégateur de flux RSS professionnel, disponible gratuitement dans sa version de base, accessible depuis un navigateur web et via application mobile. Chaque étape est accompagnée du chemin de navigation précis dans l'interface et d'une vérification permettant de confirmer le bon fonctionnement.

1) Création du compte Feedly

Se rendre sur https://feedly.com depuis le navigateur web du poste de travail GRETA. Cliquer sur « Get started for free » (bouton visible sur la page d'accueil).

Deux options d'inscription sont proposées :

- Inscription avec un compte Google (recommandée en contexte scolaire) : cliquer sur « Continue with Google » et sélectionner le compte Gmail scolaire ou personnel. Aucune création de mot de passe supplémentaire n'est requise.
- Inscription avec une adresse e-mail : cliquer sur « Continue with email », saisir l'adresse e-mail, créer un mot de passe d'au moins 8 caractères (majuscule, chiffre, caractère spécial recommandés), puis valider. Un e-mail de confirmation est envoyé : ouvrir le message et cliquer sur le lien de validation.

Une fois connecté, Feedly propose un assistant de démarrage (onboarding) suggérant des sources de contenu populaires. Cliquer sur « Skip » ou « Later » pour ignorer cet assistant et configurer manuellement les flux adaptés à la veille cybersécurité.

✓ **Vérification :** Le tableau de bord Feedly s'affiche avec le message « Your feed is empty ». La barre latérale gauche est vide. Le nom d'utilisateur ou l'adresse e-mail apparaît en bas à gauche de l'interface.

2) Découverte de l'interface Feedly

Avant d'ajouter les sources, repérer les zones principales de l'interface Feedly :

Barre latérale gauche : liste des « Feeds » (flux) et des « Collections » (dossiers thématiques). C'est ici que seront organisés les flux par thématique.

Zone centrale : liste des articles de la collection ou du flux sélectionné, avec titre, source et date de publication. Trois vues disponibles : Titre seul / Titre + extrait / Article complet.

Volet de lecture (droite, ou plein écran) : affiche le contenu de l'article sélectionné sans quitter Feedly. Il est possible de « sauvegarder » un article (icône signet) pour le retrouver plus tard.

Bouton « + Add content » : situé en bas de la barre latérale gauche. C'est le point d'entrée principal pour ajouter des flux RSS.

3) Création des collections thématiques

Dans Feedly, les flux sont organisés en « Collections » (l'équivalent des dossiers). Pour créer une collection, cliquer sur « + Add content » (barre latérale gauche) > dans le champ de recherche, saisir directement l'URL d'un flux puis, lors de la confirmation d'ajout, créer une nouvelle collection en cliquant sur « + New collection » et en lui donnant un nom.

Trois collections sont à créer pour cette veille :

- Collection 1 — Nom : « Windows / Microsoft » (contiendra les flux MSRC, Krebs on Security)
- Collection 2 — Nom : « Debian / Linux » (contiendra les flux Debian DSA, LWN.net
- Collection 3 — Nom : « Cybersécurité Générale » (contiendra les flux CERT-FR, ANSSI, NVD NIST, Krebs on Security)

Remarque : dans Feedly version gratuite, le nombre de sources est limité à 100 flux et 3 collections, ce qui est largement suffisant pour cette veille (6 sources au total).

✓ **Vérification :** Les trois collections apparaissent dans la barre latérale gauche. Elles sont encore vides à ce stade.

4) Ajout des flux RSS – Collection « Windows / Microsoft »

Cliquer sur « + Add content » en bas de la barre latérale gauche. Dans le champ « Search or enter a URL », coller l'URL du flux RSS puis appuyer sur Entrée. Feedly affiche le flux reconnu. Cliquer sur « Follow » puis, dans le menu déroulant « Add to collection », sélectionner « Windows / Microsoft ». Répéter pour chaque URL ci-dessous :

- MSRC – Security Update Guide (flux CVE officiel Patch Tuesday) : https://api.msrc.microsoft.com/update-guide/rss
- Krebs on Security – Patch Tuesday résumés et analyses CVE : https://krebsonsecurity.com/feed/

Remarque : Le flux MSRC publie les bulletins mensuels Patch Tuesday, les alertes hors-cycle (OOB) et les analyses de vulnérabilités critiques. C'est la source officielle de référence Microsoft pour les CVE Windows. Les articles apparaissent généralement le deuxième mardi de chaque mois.

✓ **Vérification :** Dans la collection « Windows / Microsoft », des articles récents du MSRC apparaissent (bulletins Patch Tuesday, analyses CVE). Le compteur d'articles non lus s'affiche à côté du nom de la collection.

5) Ajout des flux RSS – Collection « Debian / Linux »

Même procédure que l'étape 4. Cliquer sur « + Add content » > coller l'URL > Follow > Add to collection > sélectionner « Debian / Linux ».

- **Debian Security Advisories (DSA) – flux long format :** https://www.debian.org/security/dsa-long
- **LWN.net – actualités Linux et sécurité :** `https://lwn.net/headlines/rss`

Remarque : Si Feedly ne reconnaît pas directement l'URL du flux DSA Debian, essayer l'URL alternative : https://www.debian.org/security/dsa.en.rdf Le flux LWN.net peut nécessiter une souscription pour accéder aux articles complets, mais les titres et résumés sont disponibles gratuitement via le flux RSS.

✓ **Vérification :** Dans la collection « Debian / Linux », des DSA récentes apparaissent au format : « [DSA XXXX-1] nom-paquet security update ». Chaque article contient les CVE concernés et la version corrigée du paquet.

6) Ajout des flux RSS – Collection « Cybersécurité Générale »

Même procédure. Ajouter les quatre flux suivants dans la collection « Cybersécurité Générale » :

- **CERT-FR – Alertes et avis de sécurité (flux officiel français) :** https://www.cert.ssi.gouv.fr/feed/
- **NSSI – Actualités et publications :** https://www.ssi.gouv.fr/feed/
- **NVD NIST – Base nationale américaine des CVE :** https://nvd.nist.gov/feeds/xml/cve/misc/nvd-rss.xml

Remarque : Si le flux NVD NIST génère trop d'articles (plusieurs centaines par jour), il est possible de le remplacer par le flux filtré de la NVD par produit. Pour filtrer uniquement les CVE Windows : utiliser l'URL de recherche NVD avec le paramètre cpeName=cpe:/o:microsoft:windows. Le CERT-FR publie ses bulletins d'actualité hebdomadaires chaque vendredi.

✓ **Vérification :** Dans la collection « Cybersécurité Générale », les bulletins hebdomadaires du CERT-FR et les analyses de Krebs on Security apparaissent. Au total, les trois collections regroupent 6 sources actives dans Feedly.

9) Test de fonctionnement complet

Vérifier que chaque collection est active et bien alimentée :

- Cliquer sur la collection « Windows / Microsoft » : au moins 2 à 3 articles récents du MSRC ou de Microsoft Security Blog doivent être visibles.
- Cliquer sur la collection « Debian / Linux » : au moins une DSA récente (format « [DSA XXXX-1] ») doit être présente.

- Cliquer sur la collection « Cybersécurité Générale » : le dernier bulletin d'actualité du CERT-FR (CERTFR-20XX-ACT-XXX) doit apparaître.

Pour forcer une actualisation manuelle des flux : cliquer sur l'icône de rafraîchissement ↻ en haut de la collection ou actualiser la page (F5). Feedly actualise automatiquement les flux toutes les heures en version gratuite.

✓ **Vérification :** Les 6 flux RSS sont actifs, les trois collections contiennent des articles récents. Les boards « Critique », « Important » et « Veille mensuelle » sont créés et fonctionnels. La mise en place de Feedly est terminée et opérationnelle.

Résumés mensuels de veille technologique

Introduction

Ce document constitue le relevé mensuel de veille technologique réalisé sur une période de six mois (septembre 2025 – février 2026) dans le cadre du TP de veille cybersécurité BTS SIO-SISR. Chaque mois, deux articles ou bulletins de sécurité réels ont été sélectionnés parmi les sources officielles suivies (CERT-FR, MSRC, Debian Security Advisories, BleepingComputer, Krebs on Security, Tenable, Help Net Security) : un relatif à l'écosystème Microsoft/Windows, l'autre à Debian/Linux.

Pour chaque article, sont précisés : la source avec son lien hypertexte direct, la date de publication, l'identifiant CVE associé, le score CVSS, le niveau de gravité, un résumé technique et l'action recommandée.

Septembre 2025

Article 1 – Microsoft / Windows

Patch Tuesday Septembre 2025 – CVE-2025-54918 / CVE-2025-55234 : Élévations de privilèges NTLM et SMB

- **Source :** Krebs on Security – Patch Tuesday, September 2025 Edition
- **Date :** 9 septembre 2025
- **CVE :** CVE-2025-54918, CVE-2025-55234
- **CVSS :** 8.8 (Élevée) pour les deux CVE
- **Gravité :** Élevée – exploitation considérée comme probable (MSRC : "Exploitation More Likely")

Le Patch Tuesday de septembre 2025 corrige plus de 80 vulnérabilités, dont 13 critiques. Aucun zero-day activement exploité n'est signalé ce mois-ci. La CVE-2025-54918 affecte le mécanisme d'authentification Windows NTLM et permet à un attaquant distant non authentifié d'élever ses privilèges jusqu'au niveau SYSTEM. La CVE-2025-55234 touche le service Windows SMB Server : un attaquant sur le réseau peut exploiter un défaut d'authentification pour s'octroyer des droits administrateurs et potentiellement exécuter du code à distance. Près de 50 % des correctifs de ce mois concernent des élévations de privilèges, un vecteur d'attaque dominant en 2025.

Action recommandée : Appliquer les mises à jour Windows Update du 9 septembre 2025 via Windows Update ou WSUS. Activer la signature SMB (SMB Signing) et l'Extended Protection for Authentication (EPA) pour limiter les risques d'attaque par relais NTLM.

Prioriser les systèmes exposant des partages SMB ou des services d'authentification Windows sur le réseau.

Article 2 – Debian / Linux

DSA-5998-1 : CUPS – Contournement d'authentification et déni de service

- **Source :** Debian Security Advisory DSA-5998-1 – debian.org/security
- **Date :** Septembre 2025
- **CVE :** Multiples CVE (authentification bypass, déni de service)
- **CVSS :** Élevée
- **Gravité :** Élevée

Le Debian Security Team a publié la DSA-5998-1 pour CUPS (Common UNIX Printing System), le gestionnaire d'impression standard des systèmes Linux et Unix. Deux vulnérabilités ont été corrigées : un contournement d'authentification qui permet à un attaquant distant de soumettre des travaux d'impression sans s'authentifier, et une faille de déni de service qui peut provoquer le plantage du démon cupsd. Ces vulnérabilités affectent les distributions Debian 12 (Bookworm) et Debian 11 (Bullseye) et concernent tout serveur ou poste Linux disposant du service CUPS activé.

Action recommandée : Mettre à jour le paquet cups : sudo apt update && sudo apt install cups. Si CUPS n'est pas utilisé sur le système, désactiver et arrêter le service : sudo systemctl disable --now cups. Vérifier que le service n'est pas exposé sur des interfaces réseau non nécessaires.

Octobre 2025

Article 1 – Microsoft / Windows

Patch Tuesday Octobre 2025 – Record historique : 172 CVE et fin du support Windows 10

- **Source :** Krebs on Security – Patch Tuesday, October 2025 Edition + CERT-FR CERTFR-2025-ACT-017
- **Date :** 14 octobre 2025
- **CVE :** Multiples CVE dont 3 zero-days activement exploités
- **CVSS :** Jusqu'à 9.8 (Critique)
- **Gravité :** Critique – record du nombre de correctifs et fin du support Windows 10

Le Patch Tuesday d'octobre 2025 est historique : Microsoft publie 172 correctifs de sécurité, le plus grand nombre jamais émis en un seul Patch Tuesday. Parmi eux figurent trois zero-days activement exploités par des acteurs malveillants. Ce mois marque également la fin définitive du support de Windows 10 (version 22H2) le 14 octobre 2025, signalée par le CERT-FR dans son actualité CERTFR-2025-ACT-017 : à partir de cette date, aucun correctif de sécurité n'est plus publié pour Windows 10, exposant les systèmes non migrés à des risques permanents et croissants. Le CERT-FR recommande la migration vers Windows 11 ou vers une version en cycle de vie actif.

Action recommandée : Appliquer immédiatement les mises à jour cumulatives d'octobre 2025. Planifier la migration de tous les postes Windows 10 vers Windows 11 ou une version supportée. Les organisations ne pouvant migrer immédiatement peuvent souscrire au programme ESU (Extended Security Updates) de Microsoft, payant, pour obtenir un an supplémentaire de correctifs.

Article 2 – Debian / Linux

DSA-6044-1 : xorg-server – Élévation de privilèges dans le serveur X11

- **Source :** Debian Security Advisory DSA-6044-1 – debian.org/security
- **Date :** 29 octobre 2025
- **CVE :** CVE-2025-62229, CVE-2025-62230, CVE-2025-62231
- **CVSS :** Élevée
- **Gravité :** Élevée – élévation de privilèges sur serveurs X11

La DSA-6044-1 corrige trois vulnérabilités découvertes par le chercheur Jan-Niklas Sohn dans xorg-server, le serveur X11 (X Window System) utilisé sur la majorité des environnements de bureau Linux. Ces failles permettent à un attaquant local d'élever ses privilèges si le serveur X fonctionne en mode privilégié (SUID root). La mise à jour est disponible pour Debian 12 Bookworm (paquet 2:21.1.7-3+deb12u11) et Debian 13 Trixie (paquet 2:21.1.16-1.3+deb13u1).

Action recommandée : Mettre à jour xorg-server : sudo apt update && sudo apt install xserver-xorg-core. Redémarrer la session graphique après la mise à jour. Si le mode rootless (sans SUID) est utilisé, le risque est réduit mais la mise à jour reste fortement conseillée.

Novembre 2025

Article 1 – Microsoft / Windows

Patch Tuesday Novembre 2025 – Zero-day Windows exploité activement (CERT-FR CERTFR-2025-AVI-0966)

- **Source :** [CERT-FR – CERTFR-2025-AVI-0966 : Multiples vulnérabilités dans les produits Microsoft]

- **Date :** 11 novembre 2025
- **CVE :** CVE-2025-62231 et multiples CVE (novembre 2025)
- **CVSS :** Jusqu'à 9.0 (Critique)
- **Gravité :** Élevée à Critique – 1 zero-day activement exploité

Le CERT-FR publie l'avis CERTFR-2025-AVI-0966 en lien avec le Patch Tuesday de novembre 2025. Microsoft corrige plus de 60 vulnérabilités ce mois-ci, dont un zero-day activement exploité référencé dans les bulletins de sécurité MSRC publiés fin octobre et début novembre (CVE-2025-62231, CVE-2025-12060, CVE-2025-40106 entre autres). Également signalée par le CERT-FR : la CVE-2025-59287 affectant Windows Server Update Services (WSUS), publiée le 24 octobre 2025, qui permet à un attaquant de perturber le service de mises à jour des systèmes Windows en entreprise. Le CERT-FR recommande d'appliquer les correctifs dans les meilleurs délais.

Action recommandée : Appliquer les mises à jour cumulatives de novembre 2025 via Windows Update ou WSUS. Vérifier l'intégrité du service WSUS si déployé dans l'infrastructure. Consulter régulièrement le flux RSS CERT-FR (cert.ssi.gouv.fr/feed/) pour suivre les mises à jour et alertes complémentaires.

Article 2 – Debian / Linux

DSA-6053-1 : linux – Mise à jour de sécurité du noyau (multiples CVE)

- **Source :** [Debian Security Advisory DSA-6053-1 – debian.org/security]
- **Date :** 11 novembre 2025
- **CVE :** CVE-2025-21861, CVE-2025-39929, CVE-2025-39931 et nombreux autres
- **CVSS :** Élevée
- **Gravité :** Élevée – mise à jour critique du noyau Linux

La DSA-6053-1 constitue une mise à jour de sécurité majeure du noyau Linux pour Debian. Elle corrige de très nombreuses vulnérabilités, dont CVE-2025-21861, CVE-2025-39929, CVE-2025-39931, CVE-2025-39934, CVE-2025-39937 et plus d'une vingtaine d'autres CVE. Ces failles affectent divers sous-systèmes du noyau et peuvent permettre des élévations de privilèges locaux, des fuites d'informations mémoire ou des dénis de service. Cette mise à jour est disponible pour Debian 12 Bookworm et Debian 13 Trixie et concerne tous les serveurs et postes de travail Debian sous noyau standard.

Action recommandée : Mettre à jour le noyau : apt update && apt upgrade linux-image-amd64. Redémarrer obligatoirement le système après la mise à jour pour activer le nouveau noyau : sudo reboot. Vérifier la version active après redémarrage : uname -r.

Décembre 2025

Article 1 – Microsoft / Windows

Patch Tuesday Décembre 2025 – 56 CVE dont 1 zero-day exploité (dernier Patch Tuesday de l'année)

- **Source :** Krebs on Security – Patch Tuesday, December 2025 Edition
- **Date :** 9 décembre 2025
- **CVE :** Multiples CVE dont 1 zero-day activement exploité et 2 vulnérabilités divulguées publiquement
- **CVSS :** Jusqu'à 9.8 (Critique)
- **Gravité :** Élevée à Critique

Cette veille confirme l'importance de suivre des flux RSS officiels et diversifiés : le CERT-FR offre une perspective francophone et orientée risques nationaux, le MSRC fournit la référence technique Microsoft, Krebs on Security apporte une analyse d'impact et de contexte, et les DSA Debian constituent la source la plus fiable pour les systèmes Linux Debian. La combinaison de ces sources via Inoreader s'est révélée efficace pour maintenir une veille complète et réactive.

Action recommandée : Appliquer les mises à jour cumulatives de décembre 2025 (KB5072033 pour Windows 11 25H2/24H2). Vérifier si des composants React/Next.js exposés sur internet sont affectés par la CVE-2025-55182 et appliquer les mises à jour correspondantes. Consulter l'alerte CERT-FR CERTFR-2025-ALE-014 pour les indicateurs de compromission associés.

Article 2 – Debian / Linux

DSA-6073-1 : ffmpeg – Déni de service et exécution de code arbitraire

- **Source :** Debian Security Advisory DSA-6073-1 – debian.org/security
- **Date :** 7 décembre 2025
- **CVE :** CVE-2025-25473
- **CVSS :** Élevée
- **Gravité :** Élevée – traitement de fichiers multimédia malveillants

La DSA-6073-1 corrige plusieurs vulnérabilités dans FFmpeg, le framework multimédia de référence sur Linux, utilisé pour la lecture, la conversion et le streaming audio/vidéo. La CVE-2025-25473 peut provoquer un déni de service ou potentiellement l'exécution de code arbitraire lors du traitement de fichiers ou flux malformés. FFmpeg est omniprésent sur les serveurs Debian (transcodage, streaming) et postes de travail (lecture multimédia). La mise à jour est disponible en version 7:7.1.3-0+deb13u1 pour Debian 13 Trixie.

Action recommandée : Mettre à jour ffmpeg : sudo apt update && sudo apt install ffmpeg. Ne pas traiter de fichiers multimédia provenant de sources non fiables avant la mise à jour. Si FFmpeg est utilisé dans des pipelines automatisés (serveurs de transcodage), redémarrer les services concernés après la mise à jour.

Janvier 2026

Article 1 – Microsoft / Windows

Patch Tuesday Janvier 2026 – 113 CVE dont zero-day CVE-2026-20805 (DWM) et RCE Office Preview Pane

- **Source :** Krebs on Security – Patch Tuesday, January 2026 Edition
- **Date :** 14 janvier 2026
- **CVE :** CVE-2026-20805 (zero-day exploité), CVE-2026-20952, CVE-2026-20953 (RCE Office)
- **CVSS :** 8.8 (Critique) pour les RCE Office ; 5.5 pour le zero-day (activement exploité)
- **Gravité :** Critique – zero-day DWM activement exploité, RCE Office par simple prévisualisation

Microsoft corrige 113 vulnérabilités en janvier 2026, dont 8 critiques. Le zero-day CVE-2026-20805 affecte le Desktop Window Manager (DWM), composant central de l'interface graphique Windows. Bien que son score CVSS soit de 5.5, Microsoft confirme son exploitation active : ce type de faille est couramment chaîné avec une autre vulnérabilité d'exécution de code pour transformer un exploit complexe en attaque fiable et reproductible. Deux RCE critiques dans Microsoft Office (CVE-2026-20952, CVE-2026-20953) permettent l'exécution de code malveillant par simple affichage d'un message piégé dans le Volet de lecture (Preview Pane), sans ouverture explicite du fichier par l'utilisateur.

Action recommandée : Appliquer immédiatement le Patch Tuesday de janvier 2026. Désactiver le Volet de lecture d'Outlook pour les courriels provenant d'expéditeurs inconnus, en attendant la mise à jour. Surveiller les journaux Windows pour détecter toute exploitation de CVE-2026-20805 (activité anormale du processus dwm.exe).

Article 2 – Debian / Linux

DSA-6107-1 : bind9 – Déni de service sur le serveur DNS de référence Debian

- **Source :** Debian Security Advisory DSA-6107-1 – debian.org/security
- **Date :** 22 janvier 2026
- **CVE :** Multiples CVE
- **CVSS :** Élevée
- **Gravité :** Élevée – déni de service sur infrastructure DNS

La DSA-6107-1 corrige des vulnérabilités dans BIND 9 (Berkeley Internet Name Domain), le serveur DNS le plus utilisé dans les environnements Linux et l'infrastructure internet. Les failles permettent à un attaquant distant d'envoyer des requêtes malformées pour provoquer un déni de service, rendant les résolutions DNS indisponibles sur les systèmes affectés. BIND 9 est déployé sur la majorité des serveurs Debian assurant la résolution de noms en entreprise, chez les hébergeurs et dans les infrastructures réseau. Une indisponibilité DNS entraîne des coupures en cascade sur tous les services réseau qui en dépendent (web, messagerie, VPN, Active Directory).

Action recommandée : Mettre à jour bind9 : sudo apt update && sudo apt install bind9. Redémarrer le service : sudo systemctl restart named. Vérifier la configuration du resolver pour limiter les requêtes aux sources légitimes et activer les fonctions de protection contre les amplifications DNS (rate-limiting).

Février 2026

Article 1 – Microsoft / Windows

Patch Tuesday Février 2026 – 58 CVE dont 6 zero-days exploités (CVE-2026-21510 Windows Shell, CVE-2026-21514 Word)

- **Source :** Krebs on Security – Patch Tuesday, February 2026 Edition
- **Date :** 10 février 2026
- **CVE :** CVE-2026-21510 (Windows Shell), CVE-2026-21513 (MSHTML), CVE-2026-21514 (Word), CVE-2026-21519 (DWM), CVE-2026-21533 (RDP), CVE-2026-21525 (VPN DoS)
- **CVSS :** Jusqu'à 8.8 (Élevée) – 6 zero-days exploités simultanément
- **Gravité :** Critique – nombre record de zero-days exploités ce mois

Le Patch Tuesday de février 2026 corrige 58 vulnérabilités incluant six zero-days exploités activement en production, un chiffre exceptionnel. CVE-2026-21510 (Windows Shell) permet de contourner les protections Windows d'un simple clic sur un lien malveillant, affectant toutes les versions supportées de Windows. CVE-2026-21513 et CVE-2026-21514 ciblent MSHTML et Microsoft Word via des fichiers Office piégés. CVE-2026-21519 et CVE-2026-21533 permettent des élévations de privilèges dans le Desktop Window Manager et Windows Remote Desktop Services. CVE-2026-21525 provoque un déni de service dans le gestionnaire de connexions VPN Windows. Microsoft entame également le déploiement de nouveaux certificats Secure Boot pour remplacer les certificats 2011 expirant en juin 2026.

Action recommandée : Appliquer les mises à jour cumulatives de février 2026 en priorité absolue. Sensibiliser les utilisateurs à ne pas cliquer sur des liens ou ouvrir des fichiers Office provenant de sources inconnues. Restreindre l'exposition RDP sur internet et mettre en place une authentification réseau au niveau NLA (Network Level Authentication). Surveiller les certificats Secure Boot et préparer la transition vers les nouveaux certificats 2023 avant juin 2026.

Article 2 – Debian / Linux

DSA-6141-1 : linux – Mise à jour critique du noyau Debian (18 février 2026)

- **Source :** Debian Security Advisory DSA-6141-1 – debian.org/security
- **Date :** 18 février 2026
- **CVE :** Multiples CVE (noyau Linux)
- **CVSS :** Élevée
- **Gravité :** Élevée – mise à jour du noyau Linux

La DSA-6141-1, publiée le 18 février 2026, constitue la mise à jour de sécurité du noyau Linux de référence pour Debian ce mois-ci. Elle corrige plusieurs vulnérabilités affectant différents sous-systèmes du noyau, susceptibles de permettre des élévations de privilèges locaux, des fuites d'informations ou des dénis de service. Cette DSA est publiée le même jour que la DSA-6140-1 (GnuTLS) et la DSA-6139-1 (GIMP), illustrant la réactivité du Debian Security Team qui publie simultanément plusieurs mises à jour critiques en coordination avec le calendrier des éditeurs upstream. La mise à jour s'applique aux distributions Debian 12 Bookworm et Debian 13 Trixie.

Action recommandée : Mettre à jour le noyau : sudo apt update && sudo apt upgrade linux-image-amd64. Redémarrer le système pour activer le nouveau noyau : sudo reboot. Profiter de la session de maintenance pour également appliquer DSA-6140-1 (gnutls28 : sudo apt install libgnutls30) et DSA-6139-1 (gimp : sudo apt install gimp).

Synthèse :

Le tableau suivant récapitule les 12 articles réels sélectionnés sur les 6 mois, avec leur CVE et criticité.

Mois	OS	CVE principale	Gravité
Sept. 2025	Microsoft	CVE-2025-54918, CVE-2025-55234	Élevée
Sept. 2025	Debian	DSA-5998-1 (CUPS)	Élevée
Oct. 2025	Microsoft	172 CVE + fin support Win10	Critique
Oct. 2025	Debian	CVE-2025-62229/30/31 (Xorg)	Élevée
Nov. 2025	Microsoft	CVE-2025-62231 + zero-day	Élevée
Nov. 2025	Debian	DSA-6053-1 (noyau Linux)	Élevée
Déc. 2025	Microsoft	Zero-day exploité (56 CVE)	Élevée
Déc. 2025	Debian	CVE-2025-25473 (FFmpeg)	Élevée
Janv. 2026	Microsoft	CVE-2026-20805 (DWM zero-day)	Critique
Janv. 2026	Debian	DSA-6107-1 (BIND 9)	Élevée
Févr. 2026	Microsoft	6 zero-days dont CVE-2026-21510	Critique
Févr. 2026	Debian	DSA-6141-1 (noyau Linux)	Élevée

Conclusion de la veille

Sur les six mois de veille (septembre 2025 – février 2026), plusieurs tendances majeures se dégagent pour les environnements Microsoft Windows et Debian Linux. Les sources sélectionnées — MSRC, Krebs on Security, CERT-FR et Debian Security Advisories — ont fourni des informations complémentaires et cohérentes, confirmant l'intérêt d'une approche multi-sources dans la veille en cybersécurité.

Du côté Microsoft, le volume de correctifs mensuels est élevé et croissant : le record absolu de 172 CVE en octobre 2025 illustre l'ampleur de la surface d'attaque Windows. Les zero-days récurrents dans DWM (novembre 2025, janvier et février 2026), Windows Shell et les composants Office soulignent la persistance d'attaques ciblant l'interface

graphique et les suites bureautiques. La fin du support Windows 10 en octobre 2025 constitue un événement structurant qui impose une migration urgente pour les parcs informatiques encore sur cette version.

Du côté Debian, la réactivité du Security Team est remarquable : les DSA sont publiées rapidement après la divulgation des CVE upstream. Les composantes les plus fréquemment mises à jour sont le noyau Linux (DSA-6053-1 en novembre, DSA-6141-1 en février), le navigateur Chromium, les bibliothèques réseau (BIND 9, FFmpeg, CUPS) et les serveurs web. La coordination simultanée de plusieurs DSA en une même journée (comme le 18 février 2026 avec linux, gnutls28 et gimp) démontre la capacité du projet Debian à gérer des cycles de publication intensifs.

Cette veille confirme l'importance de suivre les sources officielles (MSRC, Debian DSA, CERT-FR/ANSSI).

Bilan

Conclusion :

Ce TP de veille technologique sur la cybersécurité m'a permis de découvrir et de mettre en pratique des méthodes et outils de surveillance des menaces liées aux OS Microsoft et Debian. La solution Inoreader couplée aux flux RSS officiels (CERT-FR, MSRC, DSA Debian) s'est révélée efficace pour suivre régulièrement les vulnérabilités et les correctifs.

Cette expérience m'a sensibilisé à l'importance de la veille en cybersécurité dans un contexte professionnel : un système non patché peut rapidement devenir une surface d'attaque. J'ai également pris conscience de la diversité des sources d'information disponibles et de la nécessité de privilégier les sources officielles et reconnues.

Auto-évaluation :

La configuration d'Inoreader et l'ajout des flux RSS ont été réalisés sans difficulté majeure. La partie la plus délicate a été la sélection des bonnes URLs de flux RSS, certaines sources n'étant pas toujours facilement identifiables. J'aurais pu aller plus loin en automatisant des rapports hebdomadaires depuis Inoreader.

Points d'amélioration : intégrer davantage de sources anglophones spécialisées (BleepingComputer, The Hacker News) et approfondir l'analyse des CVE avec des outils complémentaires comme Shodan ou exploit-db pour évaluer le risque réel des vulnérabilités détectées.