AYI NEDJIMI Consultants

Time-to-exploit : quand les 0-day brûlent en quelques heures

Catégorie : Cybersécurité Générale Lecture : 5 min Publié le : 26/03/2026 Auteur : Ayi NEDJIMI

En 2026, le délai d'exploitation des vulnérabilités passe de 771 jours à quelques heures. Time-to-exploit : analyse du phénomène et stratégie.

En janvier 2018, le délai moyen entre la publication d'une CVE et sa première exploitation dans la nature était de **771 jours**. En 2023, ce chiffre était tombé à **63 jours**. En mars 2026, CVE-2026-33017 sur Langflow a été exploitée 20 heures après sa divulgation publique. CVE-2026-20131 sur Cisco FMC a été exploitée 36 jours avant même sa divulgation. Nous avons franchi un seuil. Le concept de fenêtre de réponse — ce laps de temps entre la publication d'une vulnérabilité et le début de son exploitation — sur lequel repose toute la stratégie de patch management traditionnelle, est en train de disparaître. Pour les équipes de sécurité, cela signifie que les processus de remédiation construits autour de cycles de validation mensuels sont devenus structurellement incompatibles avec la réalité du threat landscape actuel. Ce n'est pas un problème de moyens, c'est un problème d'architecture de la réponse.

Ce qui a changé : l'industrialisation de l'exploitation

La réduction du time-to-exploit n'est pas un phénomène naturel. Elle est le résultat direct de l'**industrialisation des capacités offensives**. Trois facteurs se combinent aujourd'hui pour comprimer ce délai à des niveaux inédits. Premier facteur : les IA génératives permettent à des attaquants non spécialisés de développer des PoC exploitables en quelques heures à partir d'une description de vulnérabilité. Ce que cela prenait des semaines de reverse engineering peut désormais être prototype en quelques heures. Deuxième facteur : les groupes cybercriminels ont industrialisé leurs pipelines de surveillance des divulgations CVE — des bots automatiques parcourent les flux NVD, GitHub et les publications de chercheurs pour détecter et analyser les nouvelles vulnérabilités en quasi-temps-réel. Troisième facteur : les équipements de sécurité périmétrique (firewalls, VPN, load balancers) sont devenus la cible prioritaire, car leur exploitation donne accès direct aux réseaux d'entreprise. Notre analyse de CVE-2026-20131 sur Cisco FMC est un cas d'école : 36 jours d'exploitation avant la divulgation publique, sur l'équipement censé protéger le périmètre.

Le patch management traditionnel est mort

J'entends encore des RSSI qui planifient leurs cycles de patch sur des fenêtres de maintenance mensuelles. Je comprends la contrainte opérationnelle : patcher en production sans tester, c'est risquer des régressions et des interruptions de service. Mais ce raisonnement suppose qu'on dispose d'un mois pour réagir. Ce n'est plus vrai pour les CVE critiques sur les équipements

exposés. Voici les faits bruts de ce mois : CVE-2026-33017 sur Langflow — **20 heures** entre la divulgation et l'exploitation active. CVE-2025-32975 sur Quest KACE SMA — couvert dans notre analyse dédiée — exploité en moins de 48 heures. CVE-2026-22557 sur Ubiquiti UniFi — couvert dans notre article sur ce CVSS 10.0 — ciblé activement dès le lendemain de la divulgation. La fenêtre de remédiation sur les CVE critiques exposées est maintenant mesurée en heures. Le catalogue CISA KEV constitue la liste minimale des vulnérabilités à traiter en urgence.

Ce que ça implique concrètement pour les équipes défensives

La réponse ne peut pas être "patcher plus vite" — c'est nécessaire mais insuffisant. Trois axes concrets. D'abord, la réduction de la **surface d'exposition** : chaque équipement dont l'interface de management est accessible depuis Internet sans nécessité absolue est une cible potentielle. L'isolation des plans de management sur des réseaux d'administration dédiés, les bastions d'accès avec authentification forte, la suppression des accès directs non essentiels — ces mesures réduisent l'impact d'un zero-day indépendamment du patch. Ensuite, la **détection comportementale** en temps réel : si vous ne pouvez pas patcher en quelques heures, vous devez au minimum détecter l'exploitation en cours via des règles sur les comportements post-exploitation (exécution de processus enfants depuis des services web, connexions sortantes anormales, création de fichiers dans des répertoires système) plutôt que de simples signatures de CVE connues. Enfin, la **segmentation réseau** : la compromission d'un équipement périmétrique ne doit pas équivaloir à la compromission du réseau entier. Pour une mise en œuvre pratique, notre guide sur les vulnérabilités OWASP Top 10 offre un cadre applicable au renforcement de la posture défensive.

Le cas particulier des pipelines IA

CVE-2026-33017 sur Langflow n'est pas un incident isolé. Il illustre une tendance lourde : les composants d'infrastructure IA (frameworks d'agents, plateformes RAG, orchestrateurs LLM) sont devenus des cibles de premier rang, précisément parce qu'ils sont intégrés rapidement en production sans la maturité de sécurité des logiciels d'entreprise traditionnels. Notre analyse des risques de sécurité dans les pipelines IA identifiait déjà ce risque systémique. Le time-to-exploit sur ces composants sera structurellement court : les chercheurs offensifs ciblent en priorité les nouvelles surfaces d'attaque, et les pipelines IA en sont actuellement la plus dynamique.

Mon avis d'expert
Le time-to-exploit à 20 heures devrait être un signal d'alarme pour toute l'industrie. Mais je constate que la plupart des organisations continuent de gérer les CVE critiques avec les mêmes processus conçus pour un contexte où on avait des semaines pour réagir. La priorité numéro un n'est pas d'accélérer les cycles de patch — c'est de réduire la surface d'exposition et d'investir dans la détection comportementale. Un équipement de management non exposé sur Internet n'est pas affecté par CVE-2026-20131, même non patché. La meilleure défense contre une CVE critique, c'est de ne pas être exposé quand elle tombe.

Sources et références : CERT-FR · MITRE ATT&CK

Conclusion

Le time-to-exploit continuera de baisser. L'automatisation de l'analyse de vulnérabilités par les IA offensives va s'améliorer. Les attaquants les plus sophistiqués exploitent avant divulgation — c'est désormais documenté. Les stratégies défensives doivent évoluer d'une logique réactive (patch les CVE publiées) vers une logique préventive (réduire la surface exposée, détecter comportementalement, limiter l'impact par la segmentation). Ce n'est pas une question de budget, c'est une question de priorités architecturales. Et ces priorités doivent être réévaluées maintenant.

> **À retenir**
> Le time-to-exploit moyen sur les CVE critiques est passé de 771 jours en 2018 à quelques heures en 2026. Les processus de patch management mensuels sont inadaptés. La réponse : réduire la surface d'exposition, détecter comportementalement, segmenter le réseau pour limiter l'impact post-exploitation.

Comment prioriser les patchs quand le time-to-exploit est aussi court ?

Utiliser le score EPSS (Exploit Prediction Scoring System) en complément du CVSS. L'EPSS prédit la probabilité d'exploitation dans les 30 prochains jours — un CVE CVSS 10.0 avec EPSS élevé doit être traité en urgence dans les 24 heures sur les systèmes exposés. Créer deux files de traitement distinctes : la file d'urgence (CVSS >= 9.0 + exposition Internet + EPSS élevé) avec un SLA de 24-48 heures, et la file normale pour le reste. Pour les équipements impossibles à patcher rapidement, compenser par l'isolation réseau ou la mise hors ligne temporaire de l'interface exposée.

Qu'est-ce que l'EPSS et pourquoi l'utiliser en complément du CVSS ?

L'**EPSS (Exploit Prediction Scoring System)** est un modèle de machine learning publié par le FIRST qui prédit la probabilité qu'une vulnérabilité soit exploitée dans la nature dans les 30 prochains jours, sur une échelle de 0 à 1. Contrairement au **CVSS** qui mesure la sévérité théorique, l'EPSS mesure la probabilité d'exploitation réelle. Un CVE CVSS 10.0 avec EPSS 0.01 est moins urgent qu'un CVE CVSS 7.0 avec EPSS 0.85. La combinaison des deux indices permet de concentrer les efforts de patch sur les vulnérabilités réellement exploitées.

Quelles CVE 2026 ont eu le time-to-exploit le plus court ?

En 2026, les records de vitesse d'exploitation incluent : **CVE-2026-33017 (Langflow)** exploitée 20 heures après disclosure, **CVE-2026-20131 (Cisco FMC)** exploitée 36 jours avant disclosure (zero-day), **CVE-2025-32975 (Quest KACE SMA)** en moins de 48 heures. Le pattern commun : ces vulnérabilités touchent des équipements ou logiciels très répandus, sont des RCE non authentifiées, et étaient donc des cibles de choix pour les groupes offensifs équipés d'outils d'analyse automatisée.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr