AYI NEDJIMI Consultants

CVE du Mois Juin 2025 : Vulnérabilités Critiqu

6 avril 2026 • Mis à jour le 17 mai 2026 • 40 min de lecture • 10202 mots

> Analyse détaillée des vulnérabilités critiques du mois de juin 2025 : CVE W
> et IoT avec PoC, détection SIEM et remédiation.

📋 EN BREF

En bref : Ce dossier mensuel analyse en profondeur les cinq vulnérabilités les
identifiées en juin 2025. Chaque CVE est disséquée selon une méthodologie r
description technique, score CVSS v4.0, probabilité d'exploitation (EPSS), ver
concepts de preuve d'exploitation, règles de détection Sigma et stratégies de
*à titre illustratif basée sur des scénarios réalistes — les identifiants CVE utilis
fins pédagogiques.*

⚠️ ATTENTION

⚠️ **Avertissement pédagogique :** Les identifiants CVE présentés dans cet artic
CVE-2025-00005) sont **fictifs** et créés à des fins lustrer une

> rigoureuse d'analyse de vulnérabilités. Les scénarios techniques sont réalistes
> patterns d'attaque documentés. Aucun code d'exploitation fonctionnel n'est fo

Introduction : Le paysage des menaces en juin 2025

Le mois de juin 2025 s'inscrit dans une tendance préoccupante pour les équipes d
à travers le monde. Avec plus de 2 800 CVE publiées au cours des trente derniers
Vulnerability Database (NVD), les responsables de la sécurité des systèmes d'info
volume sans précédent de vulnérabilités à évaluer, prioriser et corriger. Ce flux co
d'autant plus cruciale la capacité à identifier rapidement les failles les plus danger
activement exploitées ou dont l'exploitation est imminente.

Ce mois-ci, plusieurs facteurs convergent pour créer un environnement à haut risq
campagnes de *spear phishing* ciblant les infrastructures **Active Directory** ont con
34 % par rapport au mois précédent, selon les données de threat intelligence de p
Deuxièmement, la surface d'attaque cloud continue de s'étendre avec l'adoption r
conteneurisées, exposant de nouveaux vecteurs d'exploitation. Troisièmement, l'é
reste un maillon faible, avec des firmwares dont les cycles de mise à jour sont mes
années.

Notre analyse mensuelle se concentre sur cinq vulnérabilités soigneusement séle
représentent les risques les plus significatifs pour les infrastructures d'entreprise.
l'escalade-root">escalade de privilèges dans Active Directory à l'exécution de co
conteneurs Kubernetes, en passant par des failles critiques du noyau Linux et des
dossier vous fournit les clés pour comprendre, détecter et remédier efficacement
menaces. Que vous soyez **RSSI**, administrateur système ou pentester, ces analyse
approfondies vous permettront de prioriser vos actio gement et d
sécurité de votre organisation.

Réponse sous 24h

Devis gratuit →