Authentification cassée : pourquoi 2026 ressemble à 2010

16 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 2392 mots • 19 vues •

Télécharger le PDF

> Trois CVE critiques en six semaines, trois mécanismes d'authentification cassés exactement de la même manière. Le pattern n'est plus une coïncidence : c'est un aveu collectif d'échec.

cPanel, Cisco SD-WAN, Microsoft Exchange : trois vulnérabilités critiques publiées en six semaines au printemps 2026, trois CVSS au-dessus de 9.0, trois mécanismes d'authentification cassés exactement de la même manière — des contrôles de validation insuffisants sur des flux qui auraient dû être soumis à une vérification rigoureuse depuis des années. Le pattern n'est plus une coïncidence. C'est un aveu collectif d'échec industriel. L'industrie cybersécurité a dépensé des milliards en standards d'authentification modernes — OAuth 2.0, OIDC, SAML 2.0, FIDO2, passkeys — et pendant ce temps, les produits cœur d'infrastructure continuaient de reposer sur des mécanismes de validation maison développés dans les années 2000, jamais réécrit, jamais audité avec le niveau de rigueur qu'ils méritent. 2026 ressemble à 2010 non pas parce que les attaquants ont régressé — mais parce que nos fondations de code n'ont jamais vraiment progressé.

Le retour en force de ce qu'on croyait enterré : chiffres et contexte

Pendant la première décennie des années 2010, le contournement d'authentification était le pain quotidien des CTF et des audits de sécurité des petites applications web. Les grandes plateformes, sous la pression des bug bounties et des audits de sécurité intensifs, avaient progressivement éliminé les formes les plus grossières de ces vulnérabilités. On avait appris à ne plus écrire de sessions côté serveur avant authentification, à valider les types de paramètres, à encoder correctement les sorties HTML. L'injection SQL était considérée comme l'emblème de la naïveté de développeur des années 2000.

Le printemps 2026 vient brutalement rappeler que ces leçons n'ont été apprises que par les équipes qui ont construit ex nihilo depuis 2015. Pas par les équipes qui maintiennent du code écrit en 1998 et