

# Les pannes de certificats impactent tout le monde

Selon Security Magazine, 72 % des organisations ont subi au moins une panne liée à un certificat au cours de l'année écoulée, principalement due à des certificats expirés ou invalides.

Ces incidents entraînent des interruptions de service et des risques de sécurité. La gestion du cycle de vie des certificats (CLM) permet de prévenir ces pannes en garantissant des certificats toujours valides. En automatisant la CLM, Sectigo aide les organisations à éviter les interruptions, à renforcer la sécurité et à maintenir la confiance des clients.

Voici quelques pannes récentes liées aux certificats ayant fait la une des journaux :

En savoir plus

## Spotify

286 millions d'utilisateurs actifs et jusqu'à 10 millions de clients ont été touchés par cette panne de 30 minutes.



## Microsoft Teams

Plus de 20 millions d'utilisateurs quotidiens ont été touchés, et beaucoup sont passés à Slack, le concurrent.



## Shopify

Perte directe de revenus due à la réduction du nombre de nouveaux clients acquis et à l'augmentation des coûts liés au temps passé à l'assistance clientèle.



## Fortinet

Perte directe de revenus due à la réduction du nombre de nouveaux clients acquis et à l'augmentation des coûts liés au temps passé à l'assistance clientèle.



## Xero

Plus de 3,95 millions d'abonnés ont été touchés, avec plus de 1 000 applications tierces intégrées. Le personnel des entreprises qui utilisent Xero n'a pas été payé ce mois-là.



## Google Voice

Plus de 4 heures d'indisponibilité, les clients n'ont pas pu utiliser les services ou les produits.



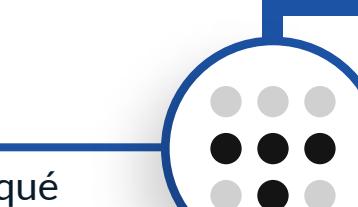
## Spotify

9 heures d'indisponibilité, aucun podcast n'était accessible.



## Tailscale.com

Un certificat expiré a provoqué une interruption de 90 minutes.



## Microsoft Azure

Une mauvaise gestion des certificats a entraîné des perturbations de service à travers les États-Unis, affectant les entreprises qui dépendent de l'infrastructure cloud de Microsoft.



## Microsoft Teams

Quelques minutes d'indisponibilité ont entraîné plusieurs heures de perturbations, de nombreux utilisateurs se tournant vers des plateformes concurrentes.



## Outlook

Bien que l'interruption n'ait duré que quelques minutes, les utilisateurs ont subi plusieurs heures de perturbations avant que les services ne reprennent normalement.



## GitHub

Des intrus ont obtenu un accès non autorisé à certains des référentiels de code de GitHub et ont volé des certificats de signature de code pour les applications GitHub Desktop et Atom.



## Cisco (Deux fois en 2023)

Plus de 20 000 clients ont été touchés par des perturbations du cloud, du stockage de données, des outils de commerce électronique et d'autres services.



## Starlink

Plusieurs heures d'indisponibilité, couvertes par les médias internationaux.



## Real Debrid

Un certificat expiré a provoqué une interruption de service de 45 minutes.



## ServiceNow

Une erreur de certificat racine a perturbé les services de plus de 600 organisations, provoquant une frustration généralisée chez les clients.



## Bank of England

Un système de paiement critique s'est effondré en raison d'un certificat expiré, provoquant une interruption de 90 minutes du CHAPS et du règlement des transactions de détail.



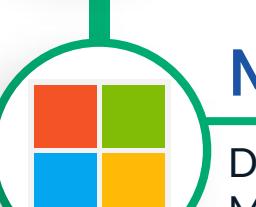
## Google Chromecast

Les appareils Chromecast ont subi une interruption de service majeure les rendant inutilisables en raison d'un certificat expiré émis en 2015 avec une validité de 10 ans.



## Starlink

Un certificat expiré a provoqué une panne mondiale qui a touché 60 000 clients. Cela s'est également produit en 2023.



## Microsoft

Divers portails de gestion Microsoft 365 et Azure ont été touchés dans le monde entier.



## League of Legends

Les joueurs n'ont pas pu se connecter pendant des heures car Riot avait oublié de renouveler le certificat SSL du client. Cela s'était également produit il y a 10 ans.

