DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 19-07-2024

BULLETIN ALERTES

Object	Panne informatique mondiale affectant les systèmes Microsoft Windows utilisant CrowdStrike.
Réference	1188
Date de Publication	2024-07-19
Sévérité	Critique

SYSTÉME AFFECTÉ :

- Les systèmes concernés qui utilisent Crowdstrike Falcon sur les systèmes Windows

DÉSCRIPTION :

Le 19 juillet 2024, CrowdStrike a connu une importante panne mondiale affectant de nombreux utilisateurs et services vitaux (aéroports, compagnies aériennes, banques, chaines de télévision, ….).

Les rapports indiquent que de nombreux utilisateurs ont été déconnectés de leurs systèmes et ont rencontré des erreurs critiques, y compris l'écran bleu de la mort (BSOD) sur les systèmes Windows

Cette panne est due à une mise à jour récente de CrowdStrike sur plusieurs systèmes Microsoft Windows. Ce problème affecte la stabilité du système et par conséquent toutes les opérations régulières.

CONTOURNEMENT PROVISOIRE :

- Démarrer Windows en mode sans échec ou dans l'environnement de récupération Windows
- Naviguer jusqu'au répertoire C:\Windows\System32\drivers\CrowdStrike
- Localiser le fichier correspondant à "C-00000291*.sys", et le supprimer.
- Démarrer l'hôte normalement.
- Identifier les systèmes concernés qui utilisent Crowdstrike Falcon sur les systèmes Windows
- Retarder les mises à jour de Crowdstrike jusqu'à l'annonce de la résolution du problème
- Restaurer le système à un point de restauration antérieur si c'est possible
- Toujours tester les mises à jour dans un environnement de test avant de les appliquer à l'environnement de production
- Toujours réaliser des sauvegardes de votre système afin de pouvoir restaurer dans le cas de problèmes similaires

DOCUMENTATION :

Le support CrowdStrike :

- https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19