Résolution du Problème CrowdStrike sur Windows

Auteur(s): Louis Ouellet

Récemment, un problème important a impliqué CrowdStrike et Microsoft Windows. Le 19 juillet 2024, CrowdStrike a publié une mise à jour de configuration de routine pour leur logiciel de capteur Falcon, ce qui a entraîné des plantages système inattendus et des écrans bleus de la mort (BSOD) sur les systèmes Windows. La mise à jour a provoqué une erreur de logique qui a corrompu des fichiers système essentiels, déclenchant des pannes généralisées dans divers secteurs, y compris la santé, la finance et les infrastructures critiques.

Environ 8,5 millions de périphériques Windows ont été affectés, représentant moins de 1 % de toutes les machines Windows dans le monde. Le problème a principalement impacté les systèmes exécutant le capteur Falcon pour Windows version 7.11 et ultérieure, qui étaient en ligne entre 04:09 UTC et 05:27 UTC le jour de la mise à jour. Le problème était particulièrement grave pour les appareils avec le chiffrement BitLocker de Windows activé, car la récupération nécessitait une clé de chiffrement souvent stockée sur des serveurs également affectés.

Pour atténuer le problème, les utilisateurs ont été invités à démarrer en Mode Sans Échec ou dans l'Environnement de Récupération de Windows et à supprimer des fichiers spécifiques corrompus du répertoire CrowdStrike. CrowdStrike a depuis annulé la mise à jour problématique et fourni des étapes de remédiation manuelle pour aider les utilisateurs touchés à restaurer leurs systèmes. Ils mènent également une analyse approfondie de la cause principale pour éviter que des incidents similaires ne se produisent à l'avenir.

Solution

1. Démarrer le système en mode sans échec
2. À l'aide d'une invite de commande ou d'une fenêtre d'explorateur, naviguez vers %windir%\System32\drivers\CrowdStrike
3. Supprimez tous les fichiers commençant par C-00000291 avec l'extension .sys
4. Redémarrez Windows en mode normal

Tagssecuritewindowscyber-sécuritécrowdstrikepannenoyau

- Twitter
- Facebook
- LinkedIn
- Reddit
- Telegram
- Email