

Type de Contenu	Description
Titre	<i>Une mise à jour de CrowdStrike provoque des pannes généralisées de Microsoft Windows.</i>
ID	202407/AS/07
Code TLP	Green
Niveau de Risque	Critique
Application et service affectés	Microsoft Windows (Azure, Microsoft 365, Teams...)
Version / Edition	Version 6.58 ou similaire
Plateforme	Microsoft WINDOWS
Mise à jour	<i>CrowdStrike a identifié un déploiement de contenu lié à ce problème et a annulé ces modifications.</i>
Résumé	<i>La panne provient d'un fichier défectueux de NCrowdStrike nommé « C-00000291*.sys ».</i>
Impacts	<ul style="list-style-type: none">- <i>Perturbations importantes pour les utilisateurs de Windows, entraînant de nombreux rapports d'erreurs d'écran bleu de la mort (BSOD).</i>- <i>Suspension ou arrêt de services</i>
Description Détaillée	<p><i>Une récente mise à jour de la société CrowdStrike a provoqué des perturbations importantes pour les utilisateurs de Windows, entraînant de nombreux rapports d'erreurs d'écran bleu de la mort (BSOD).</i></p> <p><i>Le problème semble répandu, affectant les machines exécutant différentes versions du logiciel du capteur CrowdStrike.</i></p>
Solutions	<p><i>CrowdStrike a identifié un déploiement de contenu lié à ce problème et a annulé ces modifications.</i></p> <p><i>Cette mesure devrait permettre de limiter les occurrences ultérieures des erreurs BSOD en attendant qu'une solution plus permanente soit développée. En attendant, CrowdStrike a fourni une solution de contournement aux utilisateurs confrontés à ces plantages.</i></p> <p><i>Les étapes recommandées consistent à :</i></p> <ul style="list-style-type: none">• <i>Démarrer la machine Windows concernée en mode sans échec ou dans l'environnement de récupération Windows ;</i>• <i>Accéder au répertoire C:\Windows\System32\drivers\CrowdStrike ;</i>• <i>Localiser le fichier correspondant à « C-00000291*.sys » et à le supprimer.</i>• <i>Les utilisateurs peuvent ensuite démarrer leur machine normalement.</i>
Indicateurs de Compromission	N/A

Liens pour plus
de détails

<https://gbhackers.com/crowdstrike-update-triggers-widespread/>