

We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking “Manage Cookies” at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

[MSRC](#) > [Instructions pour les clients](#) > [Guide des mises à jour de sécurité](#) > [Vulnérabilités](#) > [CVE 2021 40444](#)

Vulnérabilité d'exécution de code à distance dans Microsoft MSHTML

Sur cette page 


CVE-2021-40444
Faille de sécurité


 [Subscribe](#)  [RSS](#)  [PowerShell](#)  [API](#)

Date de publication : 7 sept. 2021

























Dernière mise à jour : 16 août 2022

Assigning CNA: Microsoft

[CVE-2021-40444](#) 

CVSS:3.0 8.8 / 7.9 

 Expand all  Collapse all

Metric	Value
 Métriques de score de base (8)	
 Vecteur d'attaque	 Réseau
 Complexité d'attaque	 Faible
 Privilèges requis	 Aucune
 Intervention de l'utilisateur	 Requise
 Étendue	 Modifiée
 Confidentialité	 Faible
 Intégrité	 Élevée
 Disponibilité	 Faible
 Métriques de score temporel (3)	
 Maturité de code malveillant	 Preuve de concept
 Niveau de correction	 Correctif officiel
 Fiabilité du rapport	 Confirmé

Pour plus d'informations sur la définition de ces métriques, consultez la page [Common Vulnerability Scoring System](#).

Synthèse

Microsoft examine des rapports signalant une vulnérabilité d'exécution de code à distance dans MSHTML qui touche Microsoft Windows. Microsoft a connaissance d'attaques ciblées visant à exploiter cette vulnérabilité en utilisant des documents Microsoft Office spécialement conçus.

Un attaquant pourrait concevoir un contrôle ActiveX malveillant à utiliser par un document Microsoft Office qui héberge le moteur de rendu de navigateur. L'attaquant devrait ensuite convaincre l'utilisateur d'ouvrir le document malveillant. Les utilisateurs dont les comptes sont configurés avec moins de droits sur le système pourraient être moins touchés que ceux qui disposent de privilèges d'administrateur.

L'antivirus Microsoft Defender et Microsoft Defender pour point de terminaison détectent la vulnérabilité connue et assurent la protection contre cette vulnérabilité. Vous devez tenir à jour les produits anti-programmes malveillants. Si vous avez activé les mises à jour automatiques, vous ne devez entreprendre aucune action supplémentaire. Si vous gérez les mises à jour dans une entreprise, vous devez sélectionner la build de détection 1.349.22.0 ou version ultérieure et la déployer dans votre environnement. Les alertes de Microsoft Defender pour point de terminaison se présentent comme suit : « Exécution de fichier Cpl suspect ».