

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](#)

AcceptRejectManage cookies

Vulnérabilité d’élévation de privilèges dans le moniteur système de Microsoft Windows (Sysmon)

CVE-2022-41120
Security Vulnerability

 Subscribe

 RSS


 PowerShell

 API

Date de publication : 8 nov. 2022

Dernière mise à jour : 22 déc. 2022

Assigning CNA: Microsoft

[CVE-2022-41120](#) 

Impact: Élévation de privilèges Gravité max.: Important

CVSS Source: Microsoft

CVSS:3.1 7.8 / 6.8 

 Expand all

 Collapse all

Metric	Value
▼ Métriques de score de base (8)	
▶ Vecteur d’attaque	▶ Locale
▶ Complexité d’attaque	▶ Faible
▶ Privilèges requis	▶ Faible
▶ Intervention de l’utilisateur	▶ Aucune
▶ Étendue	▶ Non modifié
▶ Confidentialité	▶ Élevée
▶ Intégrité	▶ Élevée
▶ Disponibilité	▶ Élevé
▼ Métriques de score temporel (3)	
▶ Maturité de code malveillant	▶ Sans preuve
▶ 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](#).

Exploitabilité

Le tableau ci-dessous fournit une [évaluation d’exploitabilité](#) pour cette vulnérabilité lors de la publication initiale.

Publicly disclosed

No

Exploited

No

Exploitability assessment