



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans Progress WS_FTP Server
<b>Numéro de Référence</b>	44010210/23
<b>Date de Publication</b>	02 Octobre 2023
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systèmes affectés

- WS\_FTP Server 2020.0.4 versions antérieures à 8.7.4
- WS\_FTP Server 2022.0.2 versions antérieures à 8.8.2

### Identificateurs externes

- CVE-2023-40044 , CVE-2023-42657 , CVE-2023-40045 , CVE-2023-40046 , CVE-2023-40047 , CVE-2023-40048 , CVE-2022-27665 , CVE-2023-40049

### Bilan de la vulnérabilité

Progress Software a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités critiques affectant les produits susmentionnés. Un attaquant pourrait exploiter ces failles afin de causer un déni de service, contourner la politique de sécurité ou exécuter du code arbitraire à distance.

### Solution

Veillez se référer au bulletin de sécurité Progress Software du 27 Septembre 2023 pour plus d'information.

### Risque

- Déni de service
- Contournement de la politique de sécurité
- Exécution du code arbitraire à distance

### Annexe

Bulletins de sécurité Progress Software du 27 Septembre 2023:

- <https://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023>