



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques dans D-Link routeur
<b>Numéro de Référence</b>	49491809/24
<b>Date de Publication</b>	18 Septembre 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systèmes affectés

- COVR-X1870 versions v1.02 et version antérieure
- DIR-X4860 versions v1.04B04\_Hot-Fix et version antérieure
- DIR-X5460 versions v1.11B01\_Hot-Fix et version antérieur

### Identificateurs externes

- CVE-2024-45694 CVE-2024-45695 CVE-2024-45696
- CVE-2024-45697 CVE-2024-45698

### Bilan de la vulnérabilité

D-Link a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités dont trois sont critiques, affectant leurs routeurs susmentionnés.

Les vulnérabilités sont les suivantes :

- CVE-2024-45694 et CVE-2024-45695 : L'exploitation réussie de la vulnérabilité pourrait permettre à un attaquant distant non authentifié d'exécuter du code arbitraire sur l'appareil affecté.
- CVE-2024-45696: L'exploitation réussie de cette vulnérabilité pourrait permettre à un attaquant distant non authentifié d'activer le service telnet et de se connecter avec des informations d'identification codées en dur.
- CVE-2024-45697: L'exploitation réussie de cette vulnérabilité pourrait permettre à un attaquant distant non authentifié d'accéder à l'appareil concerné et d'exécuter des commandes du système d'exploitation (OS) avec des informations d'identification codées en dur.
- CVE-2024-45698: L'exploitation réussie de la vulnérabilité de validation d'entrée pourrait permettre à un attaquant distant non authentifié d'accéder à telnet avec des informations d'identification codées en dur et d'exécuter des commandes arbitraires du système d'exploitation sur l'appareil affecté.

## Solution

Veillez se référer au bulletin de sécurité D-Link du 17 septembre 2024 pour plus d'information.

## Risque

- Exécution de commande à distance
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données
- Elévation de privilèges

## Annexe

Bulletins de sécurité D-Link du 17 septembre 2024:

- <https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412>