



BULLETIN DE SECURITE

| | |
|----------------------------|---|
| Titre | Vulnérabilité critique dans les produits D-Link |
| Numéro de Référence | 59780701/26 |
| Date de Publication | 07 Janvier 2026 |
| Risque | Critique |
| Impact | Critique |

Systèmes affectés

- DSL-526B <= 2.01,
- DSL-2640B <= 1.07,
- DSL-2740R < 1.17,
- DSL-2780B <= 1.01.14,

Une liste détaillée des modèles et versions potentiellement concernés sera publiée ultérieurement par D-Link.

Identificateurs externes

- CVE-2026-0625,

Bilan de la vulnérabilité

Une vulnérabilité de type injection de commandes a été identifiée dans une bibliothèque CGI compromise utilisée par plusieurs équipements DSL D-Link en fin de vie (EOL/EOS). Cette faille fait actuellement l'objet d'une exploitation active observée dans des environnements réels. L'exploitation de cette vulnérabilité peut permettre l'exécution de commandes arbitraires à distance, conduire à la compromission complète de l'équipement et faciliter son utilisation comme point d'entrée dans le réseau

Solution

Aucune mise à jour corrective ne sera publiée pour les produits EOL/EOS. D-Link recommande fortement :

- Le remplacement de toute passerelle DSL vulnérable par des équipements :
 - Toujours supportés,
 - Bénéficiant de mises à jour de sécurité régulières,
- En attendant le remplacement :

- Restreindre l'exposition réseau (désactivation de l'accès distant),
- Isoler les équipements concernés du reste du réseau.

Risque

- Elévation de privilèges,
- Exécution du code arbitraire à distance,
- Accès aux informations confidentielles,
- Prise de contrôle du système affecté,

Annexe

Bulletin de sécurité D-Link du 06 Janvier 2026:

- <https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10488>