**CYBER DEFENSE AFRICA** : ANNONCE DE SÉCURITÉ **Date** : 17/09/2024

| Type de Contenu | Description |
|---|---|
| Titre | ***Vulnérabilités critiques affectant des routeurs D-Link*** |
| ID | *202409/AS/24* |
| Code TLP | *Green* |
| Niveau de Risque | ***Critique*** |
| Application et service affectés | ***Routeurs D-Links (DIR-X5460 et DIR-X4860) Modèles A1 et COVR-X1870.*** |
| Version / Edition | *Modèle A1 versions antérieures à la version 1.04B04*<br>*Modèle COVR-X1870 versions antérieures à la version 1.03B01* |
| Plateforme | ***Routeurs D-Links.*** |
| Mise à jour | - *Mettre à jour les routeurs DIR-X5460 A1 à la version 1.11B04 ou ultérieure et le DIR-X4860 A1 à la version 1.04B05 ou ultérieure.*<br>- *Mettre à jour le firmware du COVR-X1870 à la version 1.03B01 ou ultérieure.* |
| Résumé | *Plusieurs routeurs D-Link exposés à des vulnérabilités critiques connues.* |
| Impacts | - ***Contrôle du routeur et accès non autorisé au réseau et à des données sensibles ;***<br>- ***Exécution des commandes arbitraires sur les routeurs concernés ;***<br>- ***Modification des configurations de sécurité et Installation de logiciels malveillants.*** |
| Description Détaillée | *Des millions de routeurs D-Link sont exposés à des risques de sécurité en raison de plusieurs vulnérabilités critiques. Comptabilisées au nombre de cinq (05), ces vulnérabilités critiques affectent les* ***Routeurs D-Links (DIR-X5460 ; DIR-X4860) des modèles A1 et COVR-X1870 dans leurs versions antérieures à 1.04B04 pour A1 et à version 1.03B01 pour le modèle COVR-X1870****.*<br>✓ ***Les premières vulnérabilités, CVE-2024-45694 et CVE-2024-45695,*** *affectent les modèles DIR-X5460 A1 et DIR-X4860 A1 des routeurs D-Link. Ces failles sont classées comme des vulnérabilités de débordement de mémoire tampon basée sur la pile.*<br>✓ ***La troisième vulnérabilité critique, CVE-2024-45698,*** *concerne l'injection de commandes OS par une validation d'entrée incorrecte dans le service telnet du modèle DIR-X4860 A1.*<br>✓ ***La quatrième CVE-2024-45697*** *révèle une fonctionnalité cachée dans certains routeurs D-Link où le service telnet est activé lorsque le port WAN est branché. Cette vulnérabilité affecte le modèle DIR-X4860 A1 et est classée avec un score CVSS critique de 9.8 sur une échelle de 10.*<br>✓ ***La dernière vulnérabilité, CVE-2024-45696,*** *expose des fonctionnalités cachées dans les modèles DIR-X4860 A1 et COVR-X1870. Cette vulnérabilité a un score CVSS élevé de 8.8/10 et permet aux attaquants d'activer les services telnet en envoyant des paquets spécifiques au service web et en se connectant à l'aide d'identifiants codés.*<br><br>*D-Link a publié des mises à jour urgentes pour remédier à ces risques.* |

| | |
|---|---|
| Recommandations | ***Les utilisateurs doivent appliquer les mises à jour immédiatement afin de se protéger contre les attaques potentielles pouvant provenir de l'exploitation de ces vulnérabilités.*** |
| Indicateurs de Compromission | *N/A* |
| Liens pour plus de détails | *https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412*<br>*https://www.twcert.org.tw/en/cp-139-8091-bcd52-2.html* |