AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

La faille RCE sur les routeurs D-Link exploitée par le botnet Mirai

Contenu

I. Contexte

Une nouvelle campagne de logiciels malveillants basée sur le célèbre botnet Mirai est actuellement en cours. Elle exploite activement la vulnérabilité **CVE-2025-29635**, une faille d'injection de commandes de haute criticité affectant les routeurs D-Link de la série DIR-823X. L'objectif des acteurs malveillants est d'enrôler ces appareils dans un réseau de botnets pour mener des attaques de grande ampleur.

Bien que cette faille ait été identifiée il y a plus d'un an, les experts observent aujourd'hui un changement significatif dans l'approche de ce type de campagne d'infection.

II. Analyse technique de la vulnérabilité

La faille CVE-2025-29635 permet à un attaquant distant d'exécuter des commandes arbitraires (RCE) sur les appareils cibles. En envoyant une requête POST spécifique au point de terminaison */goform/set_prohibiting*, un acteur malveillant peut déclencher l'exécution de code sans autorisation préalable.

Cette exploitation a été confirmée récemment par les chercheurs qui ont détect des tentatives d'intrusion via un réseau mondial de "honeypots" au début du mois de mars 2026. Les versions de firmware concernées sont les **240126 et 24082**.

Face à cette vulnérabilité critique, les attaquants ont mis au point une méthode d'infection structurée pour compromettre les parcs de routeurs.

III. Mode opératoire

Les observations de terrain montrent que les cybercriminels utilisent des requêtes POST pour naviguer dans les répertoires accessibles en écriture du routeur. Une fois l'accès stabilisé, ils téléchargent un script shell nommé *dlink.sh* depuis une adresse IP externe, lequel installe une variante de Mirai baptisée "tuxnokill". Ce logiciel malveillant est particulièrement polyvalent :

- Il peut infecter divers types de processeurs.
- Il intègre l'arsenal classique de Mirai, notamment les inondations TCP (SYN/ACK/STOMP), les attaques UDP et les requêtes HTTP null.

L'analyse des infrastructures de commande et de contrôle révèle que cette campagne n'est qu'un volet d'une opération plus vaste visant plusieurs constructeurs.

IV. Les cibles sont multiples

Les chercheurs ont établi que l'acteur malveillant derrière cette campagne ne se limite pas aux équipements D-Link. Le même schéma d'attaque est utilisé pour exploiter la faille **CVE-2023-1389** (affectant les routeurs TP-Link) ainsi qu'une vulnérabilité RCE distincte sur les routeurs **ZTE ZXV10 H108L**. Dans tous les cas, le but final demeure le déploiement d'une charge utile Mirai.

Le risque est d'autant plus préoccupant que les appareils D-Link visés ne bénéficient plus de support officiel.

Statut de EoL

Les routeurs de la série DIR-823X ont atteint leur fin de vie (End of Life - EoL) en novembre 2024. En conséquence, D-Link ne prévoit pas de publier de correctif pour la CVE-2025-29635, conformément à sa politique stricte concernant les produits obsolètes. le constructeur maintient généralement sa position qui stipule qu'aucun support n'est fourni une fois la date de fin de vie dépassée.

Dans ce contexte d'absence de correctif officiel, la sécurité des réseaux domestiques et professionnels repose sur des mesures préventives immédiates.

V. Recommandations de sécurité

Pour les utilisateurs d'équipements ayant atteint leur fin de vie, la persistance de ces vulnérabilités représente un danger critique. Il est impératif de suivre ces directives :

- Migrer dès que possible vers un modèle récent bénéficiant de mises à jour de sécurité régulières.
- Fermer les ports d'accès à l'interface de gestion via Internet.
- Modifier immédiatement les mots de passe administrateur par défaut.
- Inspecter vos configurations pour détecter tout changement suspect ou inhabituel.