aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité critique dans D-Link

2024-01-09 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

CVE-2016-20017

Cette vulnérabilité, affectant les routeurs D-Link DSL-2750B, est dûe à un défaut d'injection de commandes dans le paramètre *login.cgi*. Elle permet à un attaquant d'exécuter du code arbitraire.

Cette vulnérabilité est exploitée par les botnets Zerobot et Mirai.
Le CISA a ajoutée cette CVE à son référentiel de vulnérabilités exploitées (KEV), le 8 janvier 2024.

Type de vulnérabilité

- **CWE-77** : Improper Neutralization of Special Elements used in a Command ('Command Injection')

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

- Les routeurs D-Link DSL-2750B versions 1.04 et antérieures

Recommandations

- Mettre à jour les routeurs D-Link DSL-2750B vers la version 1.05 ou ultérieure.
- Des informations comlémentaires sont disponibles dans le bulletin de D-Link.

Preuve de concept

Une preuve de concept est disponible en sources ouvertes.

Références

- https://nvd.nist.gov/vuln/detail/CVE-2016-20017
- https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10088
- https://www.bleepingcomputer.com/news/security/mirai-ddos-malware-variant-expands-targets-with-13-router-exploits/
- https://www.cisa.gov/news-events/alerts/2024/01/08/cisa-adds-six-known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog