



**NATIONAL  
CSIRT CY**



**CVE-2025-4350**

**07/05/2025**

**D-Link DIR-600L wake\_on\_lan command injection**

### **CONFIDENTIAL**

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

## Executive Summary

A vulnerability classified as critical was found in D-Link DIR-600L up to 2.07B01. This vulnerability affects the function `wake_on_lan`. The manipulation of the argument `host` leads to command injection, and the attack can be initiated remotely.

## Affected versions and mitigation

The specific vulnerability affects only D-Link DIR-600L with firmware versions up to 2.07B01. To fix CVE-2025-4350, update the D-Link DIR-600L to a version beyond 2.07B01. However, this vulnerability only affects products that are no longer supported by the maintainer.

## Common Vulnerabilities & Exposures

<https://nvd.nist.gov/vuln/detail/CVE-2025-4350>

## Common Weakness Enumeration

<https://cwe.mitre.org/data/definitions/74.html>

<https://cwe.mitre.org/data/definitions/77.html>

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g. IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

## Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.