aDvens

Security for the greater good

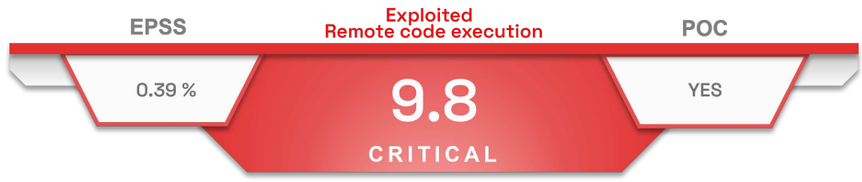
Newscast

Critical vulnerability in D-Link

2024-01-09 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

D-Link - CVE-2016-20017



This vulnerability, affecting D-Link DSL-2750B routers, is due to a command injection flaw in the *login.cgi* parameter. An attacker can exploit this to execute arbitrary code.

This vulnerability is exploited by the botnets Zerobot and Mirai.
CISA added this CVE to its exploited vulnerabilities repository (KEV) on 8 January 2024.

Type of vulnerability

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

Risk

- Remote code execution

Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Impacted Products

- D-Link DSL-2750B routers versions 1.04 and prior

Recommendations

- Update D-Link DSL-2750B routers to version 1.05 or later.
- Additional information is available in the D-Link's advisory.

Proof of concept

A proof of concept is available in open source.

Sources

- 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