aDvens

Security for the greater good

Newscast

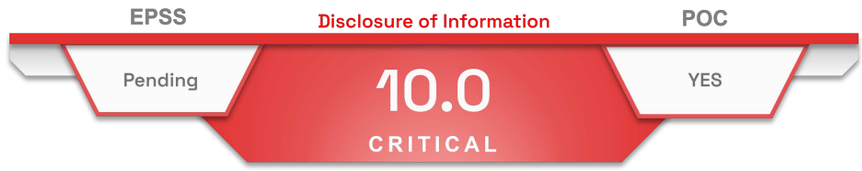
critical vulnerability in D-Link D-View

2023-12-29 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

D-LINK D-VIEW - CVE-2023-7163



On December 28, 2023, Tenable published a security advisory regarding a **critical** vulnerability affecting the network management software D-View from the manufacturer D-Link.

Security researchers from the company Tenable have identified a flaw in the validation of data entered by users in D-View.

Exploitation of this vulnerability by a remote and unauthenticated attacker allows, by manipulating the D-View manager database, to access the information of the administered probes, make them execute other tasks, and to cause a denial of service. .

Type of vulnerability

- **CWE-20**: Improper Input Validation

Risks

- Disclosure of sensitive information
- Denial of service

Criticality (CVSS v3.1 base score)

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

Product impacted

- D-Link D-View 8 version 2.0.2.89 and prior

Recommendations

There are no patch or workarounds at this time.

It is recommended to log activities to detect any suspicious behavior.

- Additional information is available at Tenable advisory.

Proof of concept

A proof of concept is available as open source.

Sources

TENABLE

- https://tenable.com/security/research/tra-2023-43

CVE-2023-7163

- https://nvd.nist.gov/vuln/detail/CVE-2023-7163