# CVE Detail – CVE-2002-1810

D-Link DWL-900AP+ Access Point 2.1 and 2.2 allows remote attackers to access the TFTP server without authentication and read the config.img file, which contains sensitive information such as the administrative password, the WEP encryption keys, and network configuration information.

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.53555

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-306: Missing Authentication for Critical Function

## CAPEC(s)

* CAPEC-12: Choosing Message Identifier
* CAPEC-166: Force the System to Reset Values
* CAPEC-216: Communication Channel Manipulation
* CAPEC-36: Using Unpublished Interfaces or Functionality
* CAPEC-62: Cross Site Request Forgery

## Affected Products

* cpe:2.3:o:dlink:dwl-900ap\+\_firmware:2.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:dlink:dwl-900ap\+\_firmware:2.2:\*:\*:\*:\*:\*:\*:\*