# CVE Detail – CVE-2020-29557

An issue was discovered on D-Link DIR-825 R1 devices through 3.0.1 before 2020-11-20. A buffer overflow in the web interface allows attackers to achieve pre-authentication remote code execution.

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.9966

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

## CAPEC(s)

* CAPEC-10: Buffer Overflow via Environment Variables
* CAPEC-100: Overflow Buffers
* CAPEC-123: Buffer Manipulation
* CAPEC-14: Client-side Injection-induced Buffer Overflow
* CAPEC-24: Filter Failure through Buffer Overflow
* CAPEC-42: MIME Conversion
* CAPEC-44: Overflow Binary Resource File
* CAPEC-45: Buffer Overflow via Symbolic Links
* CAPEC-46: Overflow Variables and Tags
* CAPEC-47: Buffer Overflow via Parameter Expansion
* CAPEC-8: Buffer Overflow in an API Call
* CAPEC-9: Buffer Overflow in Local Command-Line Utilities

## Affected Products

* cpe:2.3:o:dlink:dir-825\_r1\_firmware:\*:\*:\*:\*:\*:\*:\*:\*