# CVE Detail – CVE-2020-6078

An exploitable denial-of-service vulnerability exists in the message-parsing functionality of Videolabs libmicrodns 0.1.0. When parsing mDNS messages in mdns\_recv, the return value of the mdns\_read\_header function is not checked, leading to an uninitialized variable usage that eventually results in a null pointer dereference, leading to service crash. An attacker can send a series of mDNS messages to trigger this vulnerability.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.79598

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-252: Unchecked Return Value

## Affected Products

* cpe:2.3:a:videolabs:libmicrodns:0.1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*