# Westermo-24-11: Potential Denial of service vulnerability in WeOS

Severity **MEDIUM** 2022-11-20

## Description

WeOS utilizes several different third-party components that provide vital services to Westermo products. The component *Dnsmasq* provides DNS and DHCP services in WeOS and an issue was discovered in the component that could potentially lead to Denial-of Service of the WeOS device. The vulnerability in Dnmasq has been given the reference CVE-2023-28450

## Affected versions

Westermo products running the following WeOS operating system versions are affected

- WeOS 4 to and including 4.34
- WeOS 5 to and including 5.20.1

## Impact

An issue was discovered in Dnsmasq used in some versions of WeOS. The default maximum EDNS.0 UDP packet size was set to a value that might open for an UDP fragmentation attack. An attacker may execute a UDP Fragmentation attack against a target server to consume resources such as bandwidth and CPU resulting in Denial of Service

IP fragmentation occurs when an IP datagram is larger than the MTU of the route the datagram must traverse. Typically, the attacker will use large UDP packets over 1500 bytes of data which forces fragmentation as ethernet MTU is 1500 bytes. This attack is a variation on a typical UDP flood, but it enables more network bandwidth to be consumed with fewer packets. Additionally, it has the potential to consume server CPU resources and fill memory buffers associated with the processing and reassembling of fragmented packets.

WeOS could potentially be vulnerable to denial of service caused by a UDP Fragmentation attack. This type of attack requires the attacker to be able to generate fragmented IP traffic containing crafted data.

## Severity

| | |
|---|---|
| *Base score* | The CVSS 3.1 severity base score is 7.5 |
| *Environmental* | *The CVSS environmental score have been calculated to 4.9* |
| *Vector string* | *CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/MPR:H* |

## Mitigation

We recommend updating to the latest version of WeOS 5 to resolve the vulnerabilities mentioned in this advisory.

Additional general recommendations that reduce but not eliminates risk associated with the above vulnerabilities:

- Limit administration access from external interfaces, by e.g. disable administrative access on outward facing interfaces
- Limit administration account access to trusted parties.
- Use best practices for passwords related to administration accounts.

## Updates

The mentioned vulnerability has been mitigated in WeOS version 5.22.0, which is available for download.

## References


WeOS - Westermo Operating System ▷ Westermo https://www.westermo.com/solutions/weos

| | |
|---|---|
| CVE-2023-28450: dnsmasq | https://nvd.nist.gov/vuln/detail/CVE-2023-28450 |
| Dnsmasq | https://dnsmasq.org/doc.html |
| UDP Fragmentation | https://capec.mitre.org/data/definitions/495.html |


## Revision History

Nov 20, 2024: Initial release