



# Westermo-24-09: Security Advisory regarding RADIUS/UDP vulnerability known as “Blast-RADIUS”

CRITICAL / HIGH / MEDIUM / LOW

Last revised: 2025-03-26

Original release date: Nov 18, 2024

## Description

RADIUS is a very common protocol used for authentication, authorization, and accounting (AAA) for networked devices on enterprise and telecommunication networks. This Security Advisory discusses a vulnerability known as Blast-RADIUS, a vulnerability that may affect Westermo-products utilizing the RADIUS protocol.

RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature.

## Affected versions

Westermo products running WeOS utilizing RADIUS for authentication:

- WeOS 4 to and including version 4.34.0
- WeOS 5 to and including version 5.23.0.

Confirmed not affected

- IbexOS is not affected, as the devices enforces the requirement of a valid Message-Authenticator attribute.

## Impact

From the Blast-RADIUS description:

*“The Blast-RADIUS attack allows a man-in-the-middle attacker between the RADIUS client and server to forge a valid protocol accept message in response to a failed authentication request. This forgery could give the attacker access to network devices and services without the attacker guessing or brute forcing passwords or shared secrets. The attacker does not learn user credentials.”*

## Severity

CERT/CC coordinates the disclosure and has assigned CVE-2024-3596 and VU#456537 to this vulnerability. Since the first release of this Security Advisory NVD have published a CVSS score for CVE-2024-3596. The table below is updated accordingly. Westermo have calculated the environmental score.

Base score	The CVSS severity base score is 9.0
Environmental	-
Vector string	<a href="#">#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H</a>



## Mitigation

For WeOS 5 we recommend an upgrade to the latest WeOS 5 version. With WeOS 5.24.0 the devices enforce RADIUS to use valid Message-Authenticator attribute.

For WeOS 4 An effective approach to resolve this issue is to utilize encrypted and authenticated channels that ensure up-to-date cryptographic security protections.

Westermo layer 3 devices support VPN that can mitigate the vulnerability:

<https://docs.westermo.com/weos/weos-5/tunnels/ipsec.html#overview>

## Updates

With WeOS 5 release 5.24.0 WeOS addresses the vulnerability

For WeOS 4 there is currently no update available to address this vulnerability.

## References

RADIUS RFC 2865: <https://datatracker.ietf.org/doc/html/rfc2865>

Blast-RADIUS: <https://www.blastradius.fail/>

www.cve.org: <https://www.cve.org/CVERecord?id=CVE-2024-3596>

<https://kb.cert.org/vuls/id/456537>

CVE-2024-3596: <https://nvd.nist.gov/vuln/detail/CVE-2024-3596>

## Revision History

Nov 18, 2024: Initial release

Mar 26, 2025: Revision 1, update for WeOS 5 available