Incorrect handling of malformed packets leads to controlled buffer overflow

Critical **thebentern** published **GHSA-33hw-xhfh-944r** 4 days ago

Package	Affected versions	Patched versions
No package listed	<2.6	2.6.2

Description

Summary

A fault in the handling of mesh packets containing invalid protobuf data can result in an attacker-controlled buffer overflow, allowing an attacker to hijack execution flow, potentially resulting in remote code execution.
This attack does not require authentication or user interaction, as long as the target device rebroadcasts packets on the default channel.

This vulnerability report is subject to a 90-day responsible disclosure timeline.

Attribution: Alain Siegrist (@Alainx277) and Marc Siegrist (@MSiegrist)

Severity

Critical 9.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	Low
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

CVE ID

CVE-2025-24797

Weaknesses

CWE-119 CWE-122 CWE-787

Credits

 **Alainx277** Reporter

 **MSiegrist** Reporter

 Remediation developer
fifieldt

 Remediation develop
thebentern

 **esev** Analyst