

WESTERMO-20-01: Security Advisory

CRITICAL / HIGH / MEDIUM / LOW / INFORMATIONAL

2020-03-31

Security Vulnerability in the PPP Package

CVE

- **CVE-2020-8597**

Description

A security vulnerability in the PPP package was published 2020-03-02. It's a critical vulnerability scoring 9.8 on NIST. It might allow a remote attacker to crash parts of WeOS or even run remote code execution.

This vulnerability is most likely (unconfirmed) affecting WeOS systems configured to use PPP or more specifically "PPPoE" or "PPP over Serial Port". For more information on PPP, see WeOS Management Guide chapter 34.

Affected versions

All versions before WeOS 4.28.3

Severity

The CVSSv3 severity base score for the CVE is:

CVE-2020-8597: **9.8**

<https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H>

Mitigation

All WeOS systems explicitly configured to use PPP should be **upgraded to WeOS version 4.28.3** or greater to fix this vulnerability.

References

CVE-2020-8597 – <https://nvd.nist.gov/vuln/detail/CVE-2020-8597>