July 25, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Owl Labs' Meeting Owl Pro and Whiteboard Owl devices, the issue exists because, when in access point (AP) mode, the devices do not disconnect from the Wi-Fi network, but instead start routing all traffic to the network. This vulnerability is already being exploited in the wild

Technical Details

Owl Labs Meeting Owl and Whiteboard Owl allow attackers to activate Tethering Mode with hard-coded hoothoot credentials via a certain c 150 value.

Patches that Owl Labs started rolling out last June 22, 2022, to disable the routing of network traffic when Meeting Owl Pro and Whiteboard Owl devices are in Wi-Fi AP tethering mode, which essentially prevents their use as rogue APs.

Four other vulnerabilities in Owl Labs' devices, but these remain unpatched. The vendor said that the fix for CVE-2022-31460 should prevent exploitation attempts, but also confirmed that future updates would be addressing all issues.

The owners of Meeting Owl Pro and Whiteboard Owl video conferencing devices are advised to update to firmware as soon as possible. CISA has instructed federal agencies to address the vulnerability by June 22. 2022.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have VulnerabilityandRiskManagement@gov.bc.ca

References

- CVE-2022-31459 CVE-2022-31460 CVE-2022-31461 CVE-2022-31462 CVE-2022-31463
- Owllabs : Security vulnerabilities, CVEs (cvedetails.com)
- Owllabs NVD - Results (nist.gov)
- Threat Actors Start Exploiting Meeting Owl Pro Vulnerability Days After Disclosure - SecurityWeek
- Security Updates (owllabs.com)
- Owl Labs Update