

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



## Owl Labs Patches Severe Vulnerability in Video Conferencing Devices

By [Ionut Arghire](#) on June 08, 2022

Share

Tweet

推荐 0



Video conferencing company Owl Labs has released patches for a severe vulnerability affecting its Meeting Owl Pro and Whiteboard Owl devices.

Owl Labs' Meeting Owl Pro features a 360° lens camera to offer a panoramic view of the conference room. It offers support for various video conferencing solutions, including Zoom, Skype, and Google Meet.

Security researchers with Modzero have identified multiple vulnerabilities in Owl's devices, warning that they could be exploited to find registered devices worldwide and access sensitive data, or even gain access to the owners' networks.

The researchers discovered five vulnerabilities in Meeting Owl Pro: CVE-2022-31459, CVE-2022-31460, CVE-2022-31461 (CVSS score of 7.4), CVE-2022-31463 (CVSS score of 8.2), and CVE-2022-31462 (CVSS score of 9.3).

All of these issues, the researchers say, are [related to hardcoded credentials](#) - Meeting Owl Pro creates its own Wi-Fi access point with the hardcoded passcode "hoothoot" - and impact the communication between the Meeting Owl Pro device and its companion application and backend server, as well as the web apps used for managing Meeting Owl devices.

On Monday, Owl Labs announced the availability of patches for CVE-2022-31460, a high-severity bug that allows an attacker within Bluetooth range to turn the Meeting Owl device into a rogue access point to the owner's network.

The issue exists because, when in AP mode, the device remains connected to the Wi-Fi network and routes all traffic to the network instead of allowing only connections to the Owl itself, Modzero explains. The vulnerability can be exploited without authentication.

On Monday, Owl Labs announced firmware version 5.4.1.4 for both [Meeting Owl Pro](#) and [Whiteboard Owl](#), to disable "the passthrough of networking traffic in Wi-Fi AP tethering mode," thus preventing the use of these devices as wireless access points.

The remaining flaws, the company says, are expected to be resolved with future updates. The company also notes that all devices should be protected against potential exploitation attempts once updated to 5.4.1.4.

"To be clear, once software version 5.4.1.4 is applied, there is no risk of unauthorized network access due to the above CVEs. The Owl PIN issues are low risk and would allow someone to access per-meeting default-meeting settings only (for example: Presenter Enhance, 360-degree Pano on/off), and require them to be within Bluetooth range," the company [said](#).

The unresolved issues expose the device's internal Switchboard (allowing an attacker to perform actions supported by the companion app), and allow for access to Bluetooth-exposed functionality without authentication and for the deactivation of the passcode without authentication.

The most severe of these issues, CVE-2022-31462, is the presence of a hardcoded backdoor passcode that "can be calculated from information that is visible in Bluetooth Low Energy proximity range."

This hardcoded passcode "is the SHA-1 has representation of the devices' software serial, which is broadcasted as the name of the Owl over Bluetooth," the researchers explain.

On Tuesday, the US Cybersecurity and Infrastructure Security Agency (CISA) encouraged Owl device owners to update to firmware version 5.4.1.4.

"Owl Labs has released security updates to address a vulnerability (CVE-2022-31460) in Meeting Owl Pro and Whiteboard Owl. An attacker could exploit this vulnerability to obtain sensitive information," [CISA said](#).

**Related:** [Technical Details Released for Recently Patched Zyxel Firewall Vulnerabilities](#)

**Related:** [CISA Warns of Critical Vulnerabilities in Illumina Genetic Analysis Devices](#)

**Related:** [NSA Informs Cisco of Vulnerability Exposing Nexus Switches to DoS Attacks](#)

Share

Tweet

推荐 0



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Access Management Firm Opal Launches With \\$10 Million Series A Investment](#)

[Data Breach at Shields Health Care Group Impacts 2 Million Patients](#)

[Owl Labs Patches Severe Vulnerability in Video Conferencing Devices](#)

[SSNDOB Cybercrime Marketplace Taken Down by Law Enforcement](#)

[Whistic Raises \\$35 Million in Series B Funding for Vendor Security Network](#)