CVE-2025-1316: EDIMAX IC-7100 IP CAMERA REMOTE CODE EXECUTION VULNERABILITY

Vairav CVE Report

Date: March 07, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) has issued a critical advisory regarding a severe vulnerability (CVE-2025-1316) affecting Edimax IC-7100 IP cameras. This vulnerability allows remote code execution (RCE) through specially crafted requests, potentially giving attackers full control over affected devices. With existing public exploits, organizations using these cameras must take immediate defensive actions, as Edimax has not responded to CISA's coordination requests.

VULNERABILITY DETAILS

CVE-2025-1316: Edimax IC-7100 IP Camera RCE Vulnerability

Description: The vulnerability arises from the failure of Edimax IC-7100 cameras to neutralize incoming requests properly. An attacker can craft malicious requests to execute arbitrary code remotely, leading to full system compromise.

Impact: Remote code execution, unauthorized access, potential surveillance system hijacking.

CVSS Score: 9.8 (Critical)

AFFECTED VERSIONS

- Edimax IC-7100 IP Cameras (All known versions)

EXPLOIT DETAILS

- Public exploits for CVE-2025-1316 have already been disclosed, increasing the risk of widespread attacks.
- Exploitation requires sending specially crafted requests to the vulnerable device, enabling attackers to execute arbitrary code remotely.
- No official patches are available as Edimax has not responded to coordination efforts.

RECOMMENDED ACTIONS

Mitigation Steps:

- Ensure that affected cameras are not exposed to the internet.
- Place the devices behind firewalls and separate them from business-critical networks.

- Use VPNs for remote access, ensuring both the VPN and connected devices are up to date.
- Regularly check network logs for unusual activities associated with the cameras.
- Affected users should reach out to Edimax customer support for guidance and any potential mitigation strategies.

ADDITIONAL SECURITY MEASURES

- Disable remote administration features unless necessary.
- Use VLANs or dedicated subnets for IoT devices to limit lateral movement.
- Configure network security tools to detect and alert suspicious traffic targeting the cameras.

For Users Unable to Upgrade:

- Disable file upload functionality in WordPress where possible.
- Restrict write permissions on server directories handling user-uploaded files.
- Use security plugins to monitor and block suspicious file uploads.

REFERENCES

https://www.cve.org/CVERecord?id=CVE-2025-1316

https://securityonline.info/cisa-warns-of-critical-edimax-ip-camera-flaw-cve-2025-1316-with-public-exploits-and-no-vendor-fix/

https://www.cisa.gov/news-events/ics-advisories/icsa-25-063-08

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com