CVE-2025-20188: Cisco IOS XE Arbitrary File Upload

Vairav CVE Report

Date: May 8, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Thirbam Sadak 148
Baluwatar, Kathmandu

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical vulnerability, identified as **CVE-2025-20188**, has been discovered in Cisco IOS XE Wireless Controllers. This flaw allows unauthenticated, remote attackers to upload arbitrary files to affected systems, potentially leading to root-level remote code execution. The vulnerability has been assigned a maximum **CVSS score of 10.0**, indicating its severity. Exploitation of this vulnerability could result in complete system compromise.

VULNERABILITY DETAILS

CVE-2025-20188

- **Description:** A vulnerability exists in the web-based management interface of Cisco IOS XE Wireless Controllers. The flaw is due to the presence of hardcoded JSON Web Tokens (JWTs) that can be exploited by unauthenticated, remote attackers to upload arbitrary files to the system. This could lead to the execution of arbitrary code with root privileges.
- **Impact:** Successful exploitation allows attackers to gain root-level access, leading to complete system compromise.
- **CVSS Score:** 10.0 (Critical)

AFFECTED PRODUCTS

The following Cisco IOS XE Wireless Controllers running a vulnerable release of Cisco IOS XE Software for WLCs and have the Out-of-Band AP Image Download feature enabled are affected:

- Catalyst 9800-CL Wireless Controllers for Cloud
- Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches
- Catalyst 9800 Series Wireless Controllers
- Embedded Wireless Controller on Catalyst Access Points

EXPLOIT DETAILS

This vulnerability is particularly concerning in environments where Cisco IOS XE Wireless Controllers are deployed for network management. An unauthenticated, remote attacker can exploit the hardcoded JWTs to upload malicious files to the system, leading to arbitrary code execution with root privileges. This could result in full system compromise, allowing attackers to manipulate network configurations, intercept traffic, or disrupt services.

RECOMMENDED ACTIONS

Cisco has released software updates to address this vulnerability. Users are strongly advised to upgrade to the latest versions of Cisco IOS XE Wireless Controller software that contain the necessary patches.

ADDITIONAL SECURITY MEASURES

- Implement network segmentation to limit access to management interfaces.
- Restrict access to the web-based management interface to trusted networks and administrators.
- Monitor network traffic for unusual activities that may indicate exploitation attempts.
- Regularly audit system configurations and access controls to ensure compliance with security best practices.

REFERENCES

- https://thehackernews.com/2025/05/cisco-patches-cve-2025-20188-100-cvss.html
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC#fs
- https://app.opencve.io/cve/CVE-2025-20188

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