NATIONAL CSIRT-CY

CVE-2025-20188

Vulnerability with a CVSS score of 10.0 enables exploits in CISCO IOS XE Wireless Controller

09 May 2025

Executive Summary

CISCO has addressed a severe vulnerability denoted by its 10.0 CVSS Score via software patches. This vulnerability has been assigned with the highest possible CVSS Score.

CVE-2025-20188 concerns IOS XE Wireless Controller software.

The vulnerability allows remote attackers without authentication to obtain full root access.

This serious vulnerability only affects systems with the Out-of-Band AP Image Download feature turned on. Luckily, it is disabled by default in the configuration. But if administrators have enabled it, the systems are at high risk.

It is caused by a hardcoded JSON Web Token, that can be exploited via crafted HTTPS requests towards the Access Point image download interface. The attackers can proceed with uploading files that can execute commands in full root access, e.g. path traversal or any other arbitrary commands.

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-20188

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/798.html

Solutions

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.