Posting Date: 2025/05/22 \

[Vulnerability Alert] Cisco IOS XE Software High-Risk Security Vulnerability (CVE-2025-20188), Please Confirm and Patch Immediately

- Subject: [Vulnerability Alert] Cisco IOS XE Software High-Risk Security Vulnerability (CVE-2025-20188), Please Confirm and Patch Immediately

- Description:
  - Forwarded by National Information Sharing and Analysis Center NISAC-200-202505-00000076
  - Researchers have discovered an Arbitrary File Upload vulnerability (CVE-2025-20188) in the Out-of-Band Access Point (AP) Image Download feature of Cisco IOS XE Software for Wireless LAN Controllers (WLCs). This vulnerability allows unauthenticated remote attackers to upload backdoor programs to execute arbitrary code.
- Affected Platforms:
  - Affected Product Name: Cisco IOS XE Software with Out-of-Band AP Image Download feature enabled
  - Affected Models:
    - 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
    - Catalyst AP Embedded Wireless Controller
    - Use Cisco Software Checker (https://sec.cloudapps.cisco.com/security/center/softwarechecker.x) to verify if the current version of Cisco IOS XE Software is affected.
- Recommended Actions:
  1. Cisco has released patches for the vulnerability. Please refer to the official instructions for updates: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC
  2. If unable to update immediately, temporarily disable the Out-of-Band AP Image Download feature to prevent exploitation.
- References:
  1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC
  2. https://netmag.tw/2025/05/13/cisco-ios-xe-wireless-controller-vulnerability

---

Computing and Communication Center