Date Posted: 2025/09/30

[Vulnerability Alert] Cisco IOS XE Has a High-Risk Security Vulnerability (CVE-2025-20334)

- Subject: [Vulnerability Alert] Cisco IOS XE Has a High-Risk Security Vulnerability (CVE-2025-20334)
- Content:
  - Forwarded from Taiwan Computer Network Emergency Response Team/Coordination Center TWCERTCC-200-202509-00000014
  - Cisco has released a major security vulnerability advisory (CVE-2025-20334, CVSS: 8.8). This vulnerability exists in the HTTP API subsystem of Cisco IOS XE due to insufficient input validation, allowing an attacker with administrator privileges to authenticate to the affected system via a specially crafted API request; or allowing an unauthenticated remote attacker to induce a legitimate user with administrator privileges to click on a specially crafted link to trigger the vulnerability. If successfully exploited, the attacker may execute arbitrary commands on the affected system with root privileges.
- Affected Platforms:
  - Cisco IOS XE systems with the HTTP server feature enabled. It is recommended to check the official website for versions to determine if they are affected by this vulnerability.
  - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL#fs
- Recommended Action:
  - Please refer to the official instructions for update:
  - https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10410-5dfbf-1.html

Computer and Communications Center
Network Systems Group