POSTING DATE: 2025/12/23

[VULNERABILITY ALERT] Cisco's AsyncOS Software Contains a Critical Security Vulnerability (CVE-2025-20393)

- Subject: [VULNERABILITY ALERT] Cisco's AsyncOS Software Contains a Critical Security Vulnerability (CVE-2025-20393)

- Content Description:
  - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202512-00000009
  - AsyncOS software is an operating system specifically designed by Cisco for Cisco Secure Email Gateway, Cisco Secure Email, and Web Manager. It provides functions such as handling large volumes of email and network traffic, as well as advanced email security. Cisco has released a critical security advisory, discovering a critical security vulnerability in AsyncOS (CVE-2025-20393, CVSS: 10.0). This vulnerability allows an attacker to execute arbitrary commands with root privileges on the underlying system of affected devices. It has already been found used in cyberattack activities; for detailed solutions, please refer to the Cisco official website.
- Affected Platforms:
  - All versions of Cisco AsyncOS software are affected by this attack activity.
- Recommended Actions:
  - Patch according to the solution released on the official website: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
- Reference Material:
  - https://www.twcert.org.tw/tw/cp-169-10583-fb9f4-1.html

Computer and Communication Center
Network Systems Division, Respectfully