Date Posted: 2026/08/07

Vulnerability AlertCritical Security Vulnerability in Cisco Integrated Management Controller (CVE-2026-20200)

- Subject: Vulnerability AlertCritical Security Vulnerability in Cisco Integrated Management Controller (CVE-2026-20200)

- Description:
  - Forwarded Security Alert from TWCERT/CC (Taiwan Computer Emergency Response Team/Coordination Center) TWCERTCC-200-202608-00000003
  - Cisco Integrated Management Controller (IMC) is a management tool specifically designed for Cisco Unified Computing System (UCS) servers, providing remote server monitoring, configuration, and management capabilities. Cisco recently released a critical security advisory (CVE-2026-20200, CVSS: 8.8). This vulnerability allows an authenticated remote attacker to execute arbitrary code or commands on the underlying affected operating system and elevate privileges to root.
- Affected Platforms:
  - UCS C-Series M7 and M8 Rack Servers in standalone mode
- Recommendations:
  - Apply patches according to the solution provided on the official website: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU
- Reference Information:
  1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-20200

Computer and Communication Center
Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260807_23

Last update: **2026/08/07 09:50**