

Posted Date: 2025/06/06

[Vulnerability Alert] Privilege Escalation Vulnerability in Cisco Integrated Management Controller (CVE-2025-20261)

- Subject: [Vulnerability Alert] Privilege Escalation Vulnerability in Cisco Integrated Management Controller (CVE-2025-20261)
- Description:
 - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center TWCERTCC-200-202506-00000002
 - Cisco's Integrated Management Controller (IMC) is a management tool designed for Cisco Unified Computing System servers, providing remote monitoring, configuration, and management capabilities. A critical security vulnerability (CVE-2025-20261, CVSS: 8.8) has recently been disclosed. This vulnerability exists in the SSH connection handling and allows authenticated remote attackers to escalate privileges to access internal services.
- Affected Platforms:
 - UCS B-Series Blade Servers
 - UCS C-Series Rack Servers
 - UCS S-Series Storage Servers
 - UCS X-Series Modular System
- Recommended Actions:
 - Please refer to the official advisory for updates:
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uc-s-ssh-priv-esc-2mZDtdjM>
- References:
 - <https://www.twcert.org.tw/tw/cp-169-10165-f0f9c-1.html>

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:20250606_02



Last update: **2025/06/06 10:46**