Posting Date: 2026/04/28

[Vulnerability Alert] Two Critical Security Vulnerabilities in Cisco Integrated Management Controller

* Subject: [Vulnerability Alert] Two Critical Security Vulnerabilities in Cisco Integrated Management Controller

* Description:

- Forwarded from Taiwan Computer Emergency Response Team / Coordination Center Security Alert: TWCERTCC-200-202604-00000004.
- Cisco Integrated Management Controller (IMC) is a management tool specifically designed for Cisco Unified Computing System (UCS) servers, providing remote monitoring, configuration, and management functions. Recently, Cisco released major security advisories (CVE-2026-20093, CVSS: 9.8 and CVE-2026-20094, CVSS: 8.8).
- CVE-2026-20093 is an Authentication Bypass vulnerability that could allow an unauthenticated remote attacker to bypass authentication and access the system with administrative privileges. CVE-2026-20094 is a Command Injection vulnerability existing in the IMC Web Management Interface; an authenticated remote attacker could execute arbitrary code or commands on the underlying operating system and escalate privileges to root.

* Affected Platforms:

- Cisco 5000 Series ENCS: Versions 4.15 and earlier
- Cisco Catalyst 8300 Series Edge uCPE: Versions 4.16 and earlier
- Cisco Catalyst 8300 Series Edge uCPE: Version 4.18
- UCS C-Series M5 Rack Server: Versions 4.2 and earlier
- UCS C-Series M5 Rack Server: Version 4.3
- UCS C-Series M6 Rack Server: Versions 4.2 and earlier
- UCS C-Series M6 Rack Server: Version 4.3
- UCS C-Series M6 Rack Server: Version 6.0
- UCS E-Series M3: Versions 3.2 and earlier
- UCS E-Series M6: Versions 4.15 and earlier

* Recommended Actions:

- Apply patches according to the solutions released on the official website.
- [CVE-2026-20093] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn
- [CVE-2026-20094] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt

* References:

1. https://www.twcert.org.tw/tw/cp-169-10823-4db55-1.html

Computer and Communication Center
Network Systems Division