مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Cisco Integrated Management Controller (IMC)

Tracking #:432315779

Date:23-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity Vulnerability in Cisco Integrated Management Controller (IMC) web-based management interface that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-20356**
- CVSS Score 8.7 High
- A vulnerability exists in the Cisco Integrated Management Controller (IMC) web-based management interface that could allow an authenticated, remote attacker with Administrator-level privileges to execute arbitrary commands on the underlying operating system and potentially take full control of the affected system.

Affected Products:
This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco IMC in the default configuration:

- 5000 Series Enterprise Network Compute Systems (ENCS)
- Catalyst 8300 Series Edge uCPE
- UCS C-Series M5, M6, and M7 Rack Servers in standalone mode
- UCS E-Series Servers
- UCS S-Series Storage Servers in standalone mode

Cisco appliances that are based on a preconfigured version of one of the Cisco UCS C-Series Servers that are in the preceding list are also affected by this vulnerability if they expose access to the Cisco IMC UI.

- Application Policy Infrastructure Controller (APIC) Servers
- Business Edition 6000 and 7000 Appliances
- Catalyst Center Appliances, formerly DNA Center
- Cisco Telemetry Broker Appliance
- Cloud Services Platform (CSP) 5000 Series
- Common Services Platform Collector (CSPC) Appliances
- Connected Mobile Experiences (CMX) Appliances
- Connected Safety and Security UCS Platform Series Servers
- Cyber Vision Center Appliances
- Expressway Series Appliances
- HyperFlex Edge Nodes
- HyperFlex Nodes in HyperFlex Datacenter without Fabric Interconnect (DC-NO-FI) deployment mode
- IEC6400 Edge Compute Appliances
- IOS XRv 9000 Appliances
- Meeting Server 1000 Appliances
- Nexus Dashboard Appliances
- Prime Infrastructure Appliances

- Prime Network Registrar Jumpstart Appliances
- Secure Email Gateways1
- Secure Email and Web Manager1
- Secure Endpoint Private Cloud Appliances
- Secure Firewall Management Center Appliances, formerly Firepower Management Center
- Secure Malware Analytics Appliances
- Secure Network Analytics Appliances
- Secure Network Server Appliances
- Secure Web Appliances1
- Secure Workload Servers

Fixed Versions:
Refer Cisco advisory

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Cisco.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb