مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Cisco Integrated Management Controller

Tracking #:432315772

Date:18-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Cisco has disclosed a high-severity vulnerability in the Cisco Integrated Management Controller (IMC) affecting numerous devices.

TECHNICAL DETAILS:

Cisco has disclosed a high-severity vulnerability (**CVE-2024-20295**) in the Cisco Integrated Management Controller (IMC) affecting numerous devices. The vulnerability, which has a severity rating of **8.8** out of **10.0**, allows for unauthorized root escalation. No known exploitation has been reported as of the disclosure, but a **public release of exploit code** is available. The vulnerability impacts the Cisco Integrated Management Controller used by numerous devices.

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 Rack Servers in standalone mode
- UCS E-Series Servers

Cisco appliances that are based on a preconfigured version of a Cisco UCS C-Series Server are also affected if they expose access to the Cisco IMC CLI.

- 5520 and 8540 Wireless Controllers
- Application Policy Infrastructure Controller (APIC) Servers
- Business Edition 6000 and 7000 Appliances
- Catalyst Center Appliances, formerly DNA Center (DNAC)
- 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 Gateways
- Secure Email and Web Manager

- 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 Appliances
- Secure Workload Servers
- Telemetry Broker Appliances

Fixed Versions:
Refer Cisco advisory

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade to the latest patched version of CIMC as soon as possible.

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-mUx4c5AJ