Security Advisory 2024-042

Vulnerability in Cisco Integrated Management Controller

April 18, 2024 — v1.0

TLP:CLEAR

History:

- *18/04/2024 — v1.0 – Initial publication*

Summary

On April 17, 2024, Cisco disclosed vulnerabilities in its Cisco Integrated Management Controller product [1].

It is recommended upgrading affected products as soon as possible.

Technical Details

The vulnerability **CVE-2024-20356** [2], with a CVSS score of 8.7, could allow an authenticated, remote attacker with Administrator-level privileges to perform command injection attacks on an affected system and elevate their privileges to root. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by sending crafted commands to the web-based management interface of the affected software. A successful exploit could allow the attacker to elevate their privileges to root.

The vulnerability **CVE-2024-20295** [3], with a CVSS score of 8.8, could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have read-only or higher privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.

Affected Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco IMC in the default configuration [2,3]:

- 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. At the time of publication, this included the following Cisco products [2,3]:

- Application Policy Infrastructure Controller (APIC) Servers
- Business Edition 6000 and 7000 Appliances
- Catalyst Center Appliances, formerly DNA Center
- 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
- Telemetry Broker Appliances

Recommendations

CERT-EU recommends updating to the latest version of Cisco Integrated Management Controller as soon as possible to mitigate this vulnerability [2,3].

References

[1] https://www.bleepingcomputer.com/news/security/cisco-discloses-root-escalation-flaw-with-public-exploit-code/

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

[3] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ