BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

January 29, 2024

Critical Cisco Flaw (CVE-2024-20253)

SUMMARY

Cisco issued updates to address a severe security vulnerability affecting Unified Communications and Contact Center Solutions. This vulnerability is caused by improper handling of user-input, potentially allowing remote code execution (RCE) on a targeted device by sending a specifically crafted message to a susceptible listening port.

CVE-2024-20253 | CVSS score of 9.9.

VULNERABILITY DETAILS

The Cisco advisory stated, "...a successful exploitation of the identified vulnerability could empower an attacker to execute arbitrary commands on the underlying operating system, utilizing the privileges of the web services user". Once access to the device's operating system is achieved, the attacker could establish root access on the compromised device.

Initially discovered by Julien Egloff from Synacktiv, the flaw was found to affect various Cisco products, including:

- Unified Communications Manager (versions 11.5, 12.5(1), and 14),
- Unified Communications Manager IM & Presence Service (versions 11.5(1), 12.5(1), and 14),
- Unified Communications Manager Session Management Edition (versions 11.5, 12.5(1), and 14),
- Unified Contact Center Express (versions 12.0 and earlier, and 12.5(1)),
- Unity Connection (versions 11.5(1), 12.5(1), and 14), and
- Virtualized Voice Browser (versions 12.0 and earlier, 12.5(1), and 12.5(2)).

While there are currently no workarounds available to mitigate the vulnerability, Cisco recommends users implement access control lists (ACLs) on intermediary devices. This precautionary measure aims to restrict access by allowing communication only to the ports of deployed services. Cisco emphasized the importance of this step, especially in situations where applying the provided updates may not be immediately feasible.

RECOMMENDATIONS

- Immediately apply the patches released by Cisco to address the security flaw.
- Implement access control lists (ACLs) on intermediary devices that separate the Cisco Unified Communications or Cisco Contact Center Solutions cluster from users and the broader network.
- Deploy network monitoring tools to actively monitor and analyze network traffic.

REFERENCES

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-rce-bWNzQcUm
- https://thehackernews.com/2024/01/critical-cisco-flaw-lets-hackers.html