SecurityRisk ADVISORS

Threat Bulletin

Cisco Wireless LAN Controller Management Interface Authentication Bypass Vulnerability

Summary

On April 13, 2022, Cisco released a security advisory. The advisory details a critical vulnerability in the authentication functionality of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to bypass authentication controls and log in to the device through the management interface.

Affected Products

- 3504 Wireless Controller
- 5520 Wireless Controller
- 8540 Wireless Controller
- Mobility Express
- Virtual Wireless Controller (vWLC)
- Versions 8.10.151.4 to 8.10.151.10
- Versions 8.10.162.1 to 8.10.162.14

Safeguards/Recommendations

Affected customers are strongly encouraged to immediately apply the provided patches and mitigations. See the references below for more information regarding affected products, available patches, and the workarounds.

References

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-auth-bypass-JRNhV4fF
- https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/cmd-ref/b-cr810/config_commands_j_to_q.html#wp4097683650
- https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

Version History

Version 1. Initial Report

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io

Vendor: Cisco

CVE-ID: CVE-2022-20695

Published: Apr 13, 2022

CVSS V3 Overall score: 10.0

Criticality: Critical

Patch Availability: Yes

Vulnerability Type: Authentication Bypass

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Changed

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Not Defined

Remediation Level: Not Defined

Report Confidence: Not Defined