Security Advisory 2022-027

CISCO WLC Critical Vulnerability

April 16, 2022 — v1.0

TLP:WHITE

History:

- *16/04/2022 — v1.0 – Initial publication*

Summary

Cisco has released a security advisory to warn about a critical vulnerability (CVSS v3 score: 10.0), tracked as CVE-2022-20695, impacting the Wireless LAN Controller (WLC) software [1, 2]. A vulnerability in the authentication functionality of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to bypass authentication controls and log into the device through the management interface.

Technical Details

This vulnerability is due to the improper implementation of the password validation algorithm. An attacker could exploit this vulnerability by logging into an affected device with crafted credentials. A successful exploit could allow the attacker to bypass authentication and log into the device as an administrator. The attacker could obtain privileges that are the same level as an administrative user but it depends on the crafted credentials [1].

Affected Products

This vulnerability affects the following Cisco products if they are running Cisco WLC Software Release 8.10.151.0 or Release 8.10.162.0 and have `macfilter` radius compatibility configured as `Other`:

- 3504 Wireless Controller
- 5520 Wireless Controller
- 8540 Wireless Controller
- Mobility Express
- Virtual Wireless Controller (vWLC)

This vulnerability exists because of a non-default device configuration that must be present for it to be exploitable. To determine whether the Cisco WLC configuration is vulnerable, see [1] for details.

Recommendations

Cisco has released free software updates that address the vulnerability described in this advisory [3]. Customers with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

Workarounds

There are workarounds that address this vulnerability [1]. Choose one of the following based on the environment:

Option 1: No `macfilters` in the Environment

Customers who do not use `macfilters` can reset the `macfilter` radius compatibility mode to the default value using the following CLI command:

```
wlc > config macfilter radius-compat cisco
```

Option 2: `macfilters` in the Environment

Customers who use `macfilters` and who are able to change the radius server configuration to match other possible compatibility modes can modify the macfilter compatibility to either cisco or free using one of the following CLI commands:

```
wlc > config macfilter radius-compat cisco
wlc > config macfilter radius-compat free
```

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-auth-bypass-JRNhV4fF

[2] https://www.bleepingcomputer.com/news/security/cisco-vulnerability-lets-hackers-craft-their-own-login-credentials/

[3] https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu