National Cyber Security Centre

2204191241-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Vulnerability in Cisco Wireless LAN Controller (CVE-2022-20695)
2022-04-19

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

Cisco has disclosed a critical vulnerability in Cisco Wireless LAN controllers. The vulnerability has a CVSSv3 score of 10. The vulnerability (CVE-2022-20695) exists in devices with a non-default configuration, that allows an unauthenticated, remote attacker to bypass authentication controls and log into the management interface.

Products Affected

Cisco's advisory lists the affected software versions which are described below. However, it is important to check for the configuration that creates the vulnerability. Guidance on this can be found in the Cisco advisory.
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**":

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

Note: The vulnerable releases noted above are available in the Software Center on Cisco.com. In addition, specific customers have been given the following vulnerable escalation builds that are not in the Software Center:

- 8.10.162.1 to 8.10.162.14
- 8.10.151.4 to 8.10.151.10

Impact

CWE-303: Incorrect Implementation of Authentication Algorithm allowing Unauthorised access to infrastructure and Lateral movement through infrastructure

Mitigations

Cisco provides two workaround measures in their their advisory.

Recommendations

The NCSC recommends that organisations review the Cisco Advisory and apply patches or mitigations as soon as possible.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie