dSA211102
WPS Uses Insecure Default Setting

Published: 2021-12-16
Last updated: (initial version)
Document version: 1.0

Notice

devolo AG is aware of a security vulnerability in devolo Wi-Fi products. Exploitation of the vulnerability could allow attackers to connect to the Wi-Fi network without knowing the WPA/WPA2 key.

The information in this document is subject to change without notice and should not be construed as a commitment by devolo AG. All information that relates to the future (e.g., planned software versions and release dates) is provided without guarantee.

Affected Product and Version

- Magic 2 WiFi
- Magic 1 WiFi
- Magic 1 WiFi mini
- WiFi Repeater+ ac
- dLAN 1200+ WiFi ac
- dLAN 550+ WiFi
- dLAN 550 WiFi mini
- dLAN WiFi Outdoor

version 5.8.4 and earlier down to 5.0.0

- Magic 2 WiFi next
- Magic 2 WiFi 6

version 5.9.3 and earlier down to 5.0.0

Vulnerability Details

CWE ID: CWE-305

Description: devolo Wi-Fi devices use an insecure default for one of three WPS mechanisms. For the AP PIN method, if nothing was configured, the default is to enable the AP PIN method, using a hard-coded PIN of low complexity. That means that an attacker could brute-force the AP PIN without much effort and connect to the Wi-Fi network.

The other two WPS methods, via push-button and client PIN, are not affected.

Remediation and Mitigation

Customers are advised to update to the firmware version 5.8.5 or 5.9.4, respectively. In the new firmware the WPS method via AP PIN is disabled.

Customers are generally advised to take appropriate measures to protect access to the WLAN that the device is operated in. For sensitive networks, as mitigation WPS can be turned off until the firmware update has been installed in all devices.