Twinkly Security Advisory: Bluetooth Provisioning Vulnerability on Twinkly Light Tree 3D

Advisory ID: TWK-2025-01
Date: 08-10-2025
Affected Product Codes: See below list
Affected Firmware Version: Prior to 2.9.0
Fixed in Version: 2.9.0
CVE Reference: CVE-2025-55297
Identified by: Alexey Shalpegin, Positive Technologies

Summary

A vulnerability in the Bluetooth provisioning component could allow an attacker in close physical proximity to bypass expected authentication mechanisms during setup, potentially gaining unauthorized access. The vulnerability is only exploitable when provisioning mode has been manually re-enabled on the device; after initial setup, provisioning is disabled by default. Espressif, the vendor of the Wi-Fi module used in these products, originally provided the example provisioning code where the issue was found; our firmware has been patched according to Espressif's recommended remediations. The vulnerability was identified by Positive Technologies and responsibly coordinated.

Affected Products

The following product codes for Twinkly Light Tree 3D are affected when running firmware prior to 2.9.0:

- TWP300SPP-BEU
- TWP300SPP-BCH
- TWP300SPP-BUK
- TWP300SPP-BUS
- TWP300SPP-BAU
- TWP300SPP-BJP
- TWP500SPP-BEU
- TWP500SPP-BCH
- TWP500SPP-BUK
- TWP500SPP-BUS
- TWP500SPP-BAU
- TWP750SPP-BEU
- TWP750SPP-BUK
- TWP750SPP-BUS
- TWP750SPP-BAU
- TWP01KSPP-BEU
- TWP01KSPP-BUK
- TWP01KSPP-BUS
- TWP01KSPP-BAU
- TWP1K2SPP-BEU
- TWP1K2SPP-BUK
- TWP1K2SPP-BUS
- TWP1K2SPP-BAU

Vulnerability Details

- **CVE:** CVE-2025-55297 (Espressif advisory)
- **CWEs:** CWE-120 (Buffer Copy without Checking Size of Input) and CWE-131 (Incorrect Calculation of Buffer Size)
- **CVSS v3.1:** 5.2 (Medium) per GitHub CNA record for Espressif's advisory; we will update this page if NVD publishes its own analysis
- **Attack Vector:** Adjacent (Bluetooth range), provisioning mode must be active on the device
- **Prerequisites:** Physical access to the device and Bluetooth provisioning manually re-enabled. Firmware version below 2.9.0.

Impact

An attacker within Bluetooth range, with physical access to a device running firmware prior to 2.9.0 and provisioning mode manually re-enabled could, in an attack scenario, interfere with the provisioning exchange and potentially read memory data, compromise the device or install unauthorized firmware. There is no evidence of exploitation in real-world scenarios. Firmware version 2.9.0 removes the practical path to exploitation.

Mitigation

Firmware version 2.9.0 fully addresses this issue by:

- Patching the provisioning logic in line with Espressif's recommendations
- Improving input validation
- Reinforcing encryption during the provisioning handshake
- Adding anti-downgrade protection to prevent rollback to previous firmware versions

Secure Boot Context

The affected devices listed above inherit a known architectural limitation in Secure Boot v1, which has been previously documented in Espressif advisories such as CVE-2020-13629 and CVE-2020-15048. All newly manufactured units will include Bootloader v2, which addresses this limitation at the architectural level.

This Secure Boot v1 limitation is not considered a standalone vulnerability. It is only relevant when chained with a prior arbitrary code execution vulnerability, such as the one addressed in this advisory. As such, no new CVE is being issued for Secure Boot v1 in this context.

Credits

We thank Alexey Shalpegin and Positive Technologies for identifying and reporting the issue and for their professional cooperation throughout the coordinated disclosure process. We also thank Natalia Chichenkova for her coordination support.

Disclosure Timeline

- Initial report received: July 2025
- Firmware fix implemented: August 2025
- App rollout begins: Early September 2025
- Coordinated disclosure target date: October 8, 2025

Guidance for Users

No action is required if your device is running firmware version 2.9.0 or later. To ensure you have the latest firmware, please make sure your Twinkly App is updated to the most recent version available from the respective app store. Minimum App version supporting the updated firmware are:

- **iOS:** version 3.24.4, released on 11 September 2025.
- **Android:** version 3.24.2, released on 27 August 2025.

You can download or update the app directly from the App Store or Google Play Store. To check your firmware or manually trigger an update, please visit our support page or use the Twinkly App.

If you believe you have identified a security vulnerability, please refer to our Vulnerability Disclosure Policy or contact us securely via this form: https://help.twinkly.com/hc/en-gb/requests/new.