

WiLink WL18xx PN Reuse Issue



Summary

In certain cases, the PN used by the WL18xx firmware when transmitting packets can increment beyond the PN stored by the host-side driver for WL18xx. The host-side PN value is used to recover the system if a reset is required. If a device recovery is triggered, the PN will be restored by the value saved in the host, which can cause the WL18xx device to repeat PN numbers in subsequent transmitted packets without changing keys.

Vulnerability

TI PSIRT ID

TI-PSIRT-2021-100120

CVE ID

WiLink WL18xx PN reuse issue

CVSS Score: 5.7

CVSS Vector:

[CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H](#)

Affected Products

- WL1801, WL1831
- WL1801MOD, WL1831MOD, WL1805MOD, WL1835MOD, WL1807MOD, WL1837MOD

Potentially Impacted Features

The reuse of PN numbers can appear as a replay attack to a connected AP, which can respond by dropping incoming packets. This can lead to a period during which a WL18xx station can experience a denial of service.

Suggested Mitigations

The following updates have been released to fix this vulnerability:

- WL18xx_fw v8.9.1.0.0
- R8.8 wlcore patch: 0023-wlcore-Fixing-PN-drift-on-encrypted-link-after-recov.patch

Products based on the WL18xx NLCP Driver can be updated with the firmware version v8.9.1.0.0 and apply the wlcore patch to fix this issue.

NOTE: Both the firmware and the driver updates must be applied together for the system to work properly and to fix the issue. Updating the firmware without applying the latest driver can cause the driver to fail during initialization.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to [TI's Terms of Sale](#) or other applicable terms available either on [ti.com](https://www.ti.com) or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2023, Texas Instruments Incorporated