



# CVE-2022-45190

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-45190
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-08 00:15:00 UTC
<b>Updated</b>	2023-08-08 14:21:00 UTC
<b>Description</b>	An issue was discovered on Microchip RN4870 1.43 devices. An attacker within BLE radio range can bypass passkey entry

## Risk And Classification

**Problem Types:** CWE-306

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Microchip</a>	<a href="#">Rn4870</a>	-	All	All	All
Operating System	<a href="#">Microchip</a>	<a href="#">Rn4870 Firmware</a>	1.43	All	All	All

## References

### Reference

[BLEDiff](#) | An automated, scalable, property-agnostic, and black-box protocol noncompliance checking framework for Bluetooth Low Energy (BLE)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**