



# CVE-2021-34148

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-34148
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-09-07 07:15:00 UTC
<b>Updated</b>	2021-09-14 14:58:00 UTC
<b>Description</b>	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does not pr

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Cypress</a>	<a href="#">Cyw20735b1</a>	-	All	All	All
Operating System	<a href="#">Cypress</a>	<a href="#">Wireless Internet Connectivity For Embedded Devices</a>	All	All	All	All

## References

Reference	Source	Link	Tags
<a href="https://dl.packetstormsecurity.net/papers/general/braktooth.pdf">dl.packetstormsecurity.net/papers/general/braktooth.pdf</a>	MISC	<a href="https://dl.packetstormsecurity.net">dl.packetstormsecurity.net</a>	
CYW20735B1 Single-Chip Bluetooth Transceiver for Wireless Input Devices	MISC	<a href="https://www.cypress.com">www.cypress.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[182822](#) Debian Security Update for bluez-firmware (CVE-2021-34148)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)**