



CVE-2022-48305

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

Summary

CVE	CVE-2022-48305
State	PUBLIC
Assigner	psirt@huawei.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-27 18:15:00 UTC
Updated	2023-03-07 19:37:00 UTC
Description	There is an identity authentication bypass vulnerability in Huawei Children Smart Watch (Simba-AL00) 1.1.1.274. Successful authentication bypass allows an attacker to gain access to the device without the need for a password or PIN. The vulnerability is located in the authentication module of the device's firmware. The attack vector is local access to the device. The impact is that the attacker can gain access to the device's data and functionality. The vulnerability is rated as High severity.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Huawei	Simba-al00	-	All	All	All
Operating System	Huawei	Simba-al00 Firmware	1.1.1.274	All	All	All

References

Reference	Source	Link
Security Advisory - Identity Authentication Bypass Vulnerability in The Huawei Children Smart Watch (Simba-AL00)	MISC	www.huawei.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)