



# Hardcoded credentials in Yarbo robot firmware

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-7414
<b>State</b>	PUBLISHED
<b>Assigner</b>	AHA
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 17:15:59 UTC
<b>Updated</b>	2026-05-07 18:46:25 UTC
<b>Description</b>	Yarbo firmware v2.3.9 contains hardcoded administrative credentials embedded in the firmware image. These credentials a

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from cve@takeonme.org

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.000160000 probability, percentile 0.038210000 (date 2026-05-08)

**Problem Types:** CWE-798 | CWE-798 CWE-798 Use of Hard-coded Credentials

Version	Source	Type	Score	Severity	Vector
3.1	cve@takeonme.org	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Yarbo	Firmware	affected 2.3.9 semver	Not specified

References

Reference	Source	Lir
github.com/Bin4ry/yarbo-nat-in-my-back-yard	134c704f-9b21-4f2e-91b3-4a467353bcc0	gitl
github.com/Bin4ry/yarbo-nat-in-my-back-yard	cve@takeonme.org	gitl
takeonme.org/gcves/GCVE-1337-2026-00...	cve@takeonme.org	tak
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

Vendor Comments And Credit

Discovery Credit

**CNA:** Andreas Makris (aka Bin4ry) (en)

**CNA:** todb of AHA! (en)

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)