Hardcoded Upgrade Decryption Passwords

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-9497
State	PUBLISHED
Assigner	Microchip
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-28 11:16:35 UTC
Updated	2026-04-01 14:16:25 UTC
Description	Use of Hard-coded Credentials vulnerability in Microchip Time Provider 4100 allows Malicious Manual Software Update.Thi

Risk And Classification

Primary CVSS: v4.0 5.5 MEDIUM from dc3f6da9-85b5-4a73-84a2-2ec90b40fca5

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000050000 probability, percentile 0.002020000 (date 2026-04-01)

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

Version	Source	Type	Score	Severity	Vector
4.0	dc3f6da9-85b5-4a73-84a2-2ec90b40fca5	Secondary	5.5	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:L/VI:H/V
4.0	CNA	CVSS	5.5	MEDIUM	CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:L/VI:H/V
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

Low

Sub Conf.

Low

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

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	Microchip	Time Provider 4100	affected 2.5.0 semver	Not specified

References

Reference	Source	Link
www.microchip.com/en-us/solutions/technologies/embedded-security/how-to-report	de2f6da0-85b5-4a72-84e2-2ee00b40faa5	www.mic

www.microchip.com/en-us/solutions/technologies/embedded-security/how-to-report-...	dc3f6da9-85b5-4a73-84a2-2ec90b40fca5	www.mic
www.gruppotim.it/en/footer/TIM-red-team.html	dc3f6da9-85b5-4a73-84a2-2ec90b40fca5	www.gru
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Dario Emilio Bertani (en)

CNA: Raffaele Bova (en)

CNA: Andrea Sindoni (en)

CNA: Simone Bossi (en)

CNA: Antonio Carriero (en)

CNA: Marco Manieri (en)

CNA: Vito Pistillo (en)

CNA: Davide Renna (en)

CNA: Manuel Leone (en)

CNA: Massimiliano Brolli (en)

CNA: TIM Security Red Team Research (TIM S.p.A) (en)

Additional Advisory Data

Workarounds

CNA: Upgrades are only available on a separate management port which should not be connected to an untrusted network. ACLs are available to further restrict access to only trusted addresses.

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