RCE on backup configuration password

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-47900
State	PUBLISHED
Assigner	Microchip
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-20 18:15:38 UTC
Updated	2026-03-31 11:16:12 UTC
Description	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Microchip T

Risk And Classification

Primary CVSS: v4.0 8.9 HIGH from dc3f6da9-85b5-4a73-84a2-2ec90b40fca5

CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/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: 0.003920000 probability, percentile 0.601010000 (date 2026-04-01)

Problem Types: CWE-78 | CWE-78 CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
4.0	dc3f6da9-85b5-4a73-84a2-2ec90b40fca5	Secondary	8.9	HIGH	CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H
4.0	CNA	CVSS	8.9	HIGH	CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Microchip	Timeprovider 4100	-	All	All	All
Operating System	Microchip	Timeprovider 4100 Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Microchip	Time Provider 4100	affected 2.5 semver	Not specified

References

Reference	Source	Link
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.grup
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: Do not expose the web interface on the separate management port to an untrusted network. For added security, users have the option to disable the web interface, further protecting the device from potential web-based exploitations.

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

CVE.report and Source URL Uptime Status status.cve.report