



# RCE on backup configuration password

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

## Summary

<b>CVE</b>	CVE-2025-47900
<b>State</b>	PUBLISHED
<b>Assigner</b>	Microchip
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-10-20 18:15:38 UTC
<b>Updated</b>	2026-03-31 11:16:12 UTC
<b>Description</b>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Microchip

## 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/MSX/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/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
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

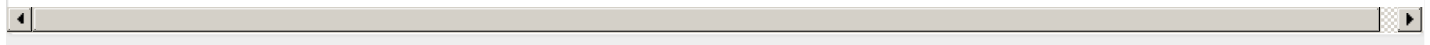
Low

User Interaction

None

**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/MSX/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	<a href="#">Microchip</a>	<a href="#">Time Provider 4100</a>	affected 2.5 semver	Not specified
-----	---------------------------	------------------------------------	---------------------	---------------

## References

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

## 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.

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**