Weak credentials vulnerability in the CashDro 3 web administration panel

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-8076
State	PUBLISHED
Assigner	INCIBE
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 12:16:29 UTC
Updated	2026-05-08 15:51:08 UTC
Description	Weak credentials in the CashDro 3 web administration panel, version 24.01.00.26, where the platform allows the use of nur

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from cve-coordination@incibe.es

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/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: 0.000670000 probability, percentile 0.206270000 (date 2026-05-12)

Problem Types: CWE-1391 | CWE-1391 CWE-1391: Use of Weak Credentials

Version	Source	Type	Score	Severity	Vector
4.0	cve-coordination@incibe.es	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CashDro	CashDro 3 Administration Panel	affected 24.01.00.26	Not specified

References

Reference	Source	Link	Tags
www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-cashdro-3	cve-coordination@incibe.es	www.incibe.es	
labs.itresit.es/2026/05/07/cashdro-vulnerabilities-from-pentest-to-stealing-m...	cve-coordination@incibe.es	labs.itresit.es	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

Vendor Comments And Credit

Discovery Credit

CNA: Pedro Gabaldón Juliá (en)

CNA: Javier Medina Munuera (en)

CNA: David Montoro Aguilera (en)

CNA: Javier Ayala Ortín (en)

CNA: Pedro Castillo Torío (en)

Additional Advisory Data

Solutions

CNA: The new versions of Cashdro support alphanumeric PINs, thereby addressing the first

vulnerability.

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

Free CVE JSON API cve.report/api

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