CVE-2026-4832

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

Summary

CVE	CVE-2026-4832
State	PUBLISHED
Assigner	schneider
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 16:16:48 UTC
Updated	2026-04-17 15:11:35 UTC
Description	CWE-798 Use of Hard-coded Credentials vulnerability exists that could cause unauthorized access to sensitive device infor

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from cybersecurity@se.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/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: 0.000780000 probability, percentile 0.232630000 (date 2026-04-21)

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

Version	Source	Type	Score	Severity	Vector
4.0	cybersecurity@se.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

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:L/VI:N/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	Platfo
CNA	Schneider Electric	Easergy MiCOM P14x	affected All versions prior to B4A	Not sp
CNA	Schneider Electric	Easergy MiCOM P24x	affected All versions prior to D3A	Not sp
CNA	Schneider Electric	Easergy MiCOM P341	affected All versions prior to E3F	Not sp
CNA	Schneider Electric	Easergy MiCOM P342 P343 P344 P345	affected All versions prior to B3F	Not sp
CNA	Schneider Electric	Easergy MiCOM P442 P444	affected All versions prior to E3A	Not sp
CNA	Schneider Electric	Easergy MiCOM P443 P445 P446 P543 P544 P545 P546	affected All versions prior to H6A	Not sp
CNA	Schneider Electric	Easergy MiCOM P642 P645	affected All versions prior to B4A	Not sp
CNA	Schneider Electric	Easergy MiCOM P643	affected All versions prior to B3F	Not sp
CNA	Schneider Electric	Easergy MiCOM P741 P742 P743	affected All versions prior to B2A	Not sp
CNA	Schneider Electric	Easergy MiCOM P746	affected All versions prior to B4E or C4E	Not sp
CNA	Schneider Electric	Easergy MiCOM P841	affected All versions prior to G6A	Not sp
CNA	Schneider Electric	Easergy MiCOM P849	affected All versions prior to B4A	Not sp

References

Reference	Source	Link	Tags
download.schneider-electric.com/files	cybersecurity@se.com	download.schneider-electric.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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