Subnet Solutions PowerSYSTEM Center Incorrect Authorization

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

Summary

CVE	CVE-2026-33570
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 22:16:33 UTC
Updated	2026-05-12 22:16:33 UTC
Description	PowerSYSTEM Center REST API endpoint for devices allows a low privilege authenticated user to access information norn

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from ics-cert@hq.dhs.gov

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/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

Problem Types: CWE-863 | CWE-863 CWE-863 Incorrect Authorization

Version	Source	Type	Score	Severity	Vector
4.0	ics-cert@hq.dhs.gov	Secondary	6.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/
4.0	CNA	CVSS	6.9	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
3.1	ics-cert@hq.dhs.gov	Secondary	5.7	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	5.7	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

None

Confidentiality

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/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

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Subnet Solutions	PowerSYSTEM Center 2020	affected 5.11.x 5.28.x custom	Not specified

References

Reference	Source	Link	Tags
www.cisa.gov/news-events/ics-advisories/icsa-26-132-02	ics-cert@hq.dhs.gov	www.cisa.gov	

github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2026/icsa-26-13...	ics-cert@hq.dhs.gov	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Kelly Stich of Subnet Solutions Inc. reported these vulnerabilities to CISA. (en)

Additional Advisory Data

Solutions

CNA: Subnet Solutions recommends users update to the latest version of PowerSYSTEM Center PSC 2020 Update 29, PSC 2024 Update 2, and PSC 2026 GA Hotfix. For assistance in upgrading, users should contact a Subnet Solutions System Integration team member or customer support team at (403) 270-8885 or by email at support@subnet.com. Subnet Solutions recommends users do the following in order to reduce risk: * Monitor user activity records to ensure users are following acceptable usage policies of the application. * Restrict access to Notification Settings to trusted Administrators Monitor "Send from Address" in settings and Activity Records. * Configure a notification rule that triggers in any bulk account export activity.

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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 registred 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.

Free CVE JSON API cve.report/api

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