



# CVE-2026-2402

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

## Summary

<b>CVE</b>	CVE-2026-2402
<b>State</b>	PUBLISHED
<b>Assigner</b>	schneider
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 16:16:38 UTC
<b>Updated</b>	2026-04-22 14:11:43 UTC
<b>Description</b>	CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists that would allow an attacker to gain

## 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:N/VI:N/VA:L/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000590000 probability, percentile 0.184840000 (date 2026-04-21)

**Problem Types:** CWE-307 | CWE-307 CWE-307 Improper Restriction of Excessive Authentication Attempts

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:N/VI:N/VA:L/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:N/VI:N/VA:L/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Attack Requirements

**None**

Privileges Required

**None**

User Interaction

**None**

Confidentiality: None

Integrity: None

Availability: Low

Sub Conf.: None

Sub Integrity: None

Sub Availability: None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/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/MSG: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: None

User Interaction: None

Scope: Unchanged

Confidentiality: None

Integrity: None

Availability: Low

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	Powerchute Serial Shutdown	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Schneider Electric	PowerChute Serial Shutdown	affected Versions v1.4 and prior	Not specified

## References

Reference	Source	Link	Tags
<a href="https://download.schneider-electric.com/files">download.schneider-electric.com/files</a>	<a href="mailto:cybersecurity@se.com">cybersecurity@se.com</a>	<a href="https://download.schneider-electric.com">download.schneider-electric.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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 registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)