

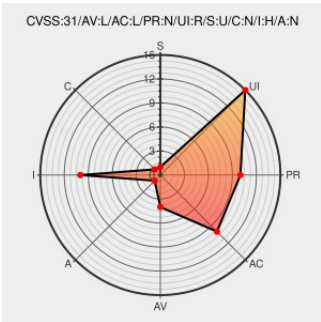


CVE-2022-40976

Published on: Not Yet Published

Last Modified on: 11/25/2022 01:59:00 PM UTC

CVE-2022-40976 - advisory for VDE-2022-044

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF !\[\]\(faf942dc3e59ce8eb64b4ac481eca7e0_img.jpg\)](#)

Certain versions of **PAScal** from **PILZ** contain the following vulnerability:

A path traversal vulnerability was discovered in multiple Pilz products. An unauthenticated local attacker could use a zipped, malicious configuration file to trigger arbitrary file writes ('zip-slip').

CVE-2022-40976 has been assigned by [cert info@cert.vde.com](mailto:info@cert.vde.com) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVE References

Description	Tags	Link
VDE-2022-045 CERT@VDE	cert.vde.com text/html	cert MISC cert.vde.com/en/advisories/VDE-2022-045/
VDE-2022-044 CERT@VDE	cert.vde.com text/html	cert MISC cert.vde.com/en/advisories/VDE-2022-044/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.


There are currently no QIDs associated with this CVE

Known Affected Software

Vendor	Product	Version
PILZ	PAScal	= 1.0.0
PILZ	PASconnect	= 1.0.0
PILZ	PASmotion	= 1.0.0
PILZ	PNOZmulti_Configurator	= 1.0.0
PILZ	PNOZmulti_Configurator_LTS	= 1.0.0
PILZ	PAS4000	= 1.0.0

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-40976 : A path traversal vulnerability was discovered in multiple Pilz products. An unauthenticated local... twitter.com/i/web/status/1...	2022-11-24 10:05:54
 /r/netcve	CVE-2022-40976	2022-11-24 11:38:20

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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](#) 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