



# Wago: Vulnerability in WBM through Open VPN

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

## Summary

<b>CVE</b>	CVE-2024-1490
<b>State</b>	PUBLISHED
<b>Assigner</b>	CERTVDE
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-09 11:16:19 UTC
<b>Updated</b>	2026-04-13 15:02:47 UTC
<b>Description</b>	An authenticated remote attacker with high privileges can exploit the OpenVPN configuration via the web-based management interface.

## Risk And Classification

**Primary CVSS:** v3.1 7.2 HIGH from info@cert.vde.com

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

**EPSS:** 0.000960000 probability, percentile 0.265280000 (date 2026-04-15)

**Problem Types:** CWE-94 | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	info@cert.vde.com	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WAGO	CC100 0751-9x01	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	PFC100 G1 0750-810-xxxx-xxxx	affected 0.0.0 3.10.10 semver	Not specified
CNA	WAGO	PFC100 G2 0750-811x-xxxx-xxxx	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	PFC200 G1 750-820x-xxxx-xxxx	affected 0.0.0 3.10.10 semver	Not specified
CNA	WAGO	PFC200 G2 750-821x-xxxx-xxxx	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	TP600 0762-420x-8000-000x	affected 0.0.0 FW 26 semver	Not specified
CNA	WAGO	TP600 0762-430x-8000-000x	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	TP600 0762-520x-8000-000x	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	TP600 0762-530x-8000-000x	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	TP600 0762-620x-8000-000x	affected 0.0.0	Not specified
CNA	WAGO	TP600 0762-630x-8000-000x	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	Edge Controller 0752-8303-8000-0002	affected 0.0.0 4.5.10 semver	Not specified
CNA	WAGO	WP400 0762-340x	affected 0.0.0 4.5.10 semver	Not specified

### References

Reference	Source	Link	Tags
certvde.com/de/advisories/VDE-2024-008	info@cert.vde.com	<a href="https://certvde.com">certvde.com</a>	
wago.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2024-008.json	info@cert.vde.com	<a href="https://wago.csaf-tp.certvde.com">wago.csaf-tp.certvde.com</a>	
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, anal

### Vendor Comments And Credit

Discovery Credit

**CNA:** Jeroen Wijenbergh, Floris Hendriks from Radboud University (en)

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 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](#).

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

**CVE.report and Source URL Uptime Status** [status.cve.report](#)