



Permissive Web Security Policy Allows Cross-Origin Access Control Bypass on Omada Cloud Controllers

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

Summary

CVE	CVE-2025-9292
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-13 02:16:45 UTC
Updated	2026-04-01 20:52:43 UTC
Description	A permissive web security configuration may allow cross-origin restrictions enforced by modern browsers to be bypassed u

Risk And Classification

Primary CVSS: v4.0 2 LOW from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000170000 probability, percentile 0.038360000 (date 2026-04-01)

Problem Types: CWE-942 | CWE-942 CWE-942 Permissive Cross-domain Security Policy with Untrusted Domains

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	2	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

High

User Interaction

Passive

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:P/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/MS:C: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

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tp-link	Aginet	All	All	All	All
Application	Tp-link	Deco	All	All	All	All
Application	Tp-link	Festa	All	All	All	All

Application	Tp-link	Kasa	All	All	All	All
Application	Tp-link	Kidshield	All	All	All	All
Application	Tp-link	Omada	All	All	All	All
Application	Tp-link	Omada Guard	All	All	All	All
Application	Tp-link	Tapo	All	All	All	All
Application	Tp-link	Tether	All	All	All	All
Application	Tp-link	Tp-partner	All	All	All	All
Application	Tp-link	Tpcamera	All	All	All	All
Application	Tp-link	Vigi	All	All	All	All
Application	Tp-link	Wi-fi Navi	All	All	All	All
Application	Tp-link	Wifi Toolkit	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	Omada Cloud Controller	affected custom	Omada

References

Reference	Source	Link	Tags
www.tp-link.com/us/support/faq/4969	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Vendor Advisory
www.omadanetworks.com/us/support/faq/4969	f23511db-6c3e-4e32-a477-6aa17d310630	www.omadanetworks.com	Vendor Advisory
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: [Francesco La Spina, Stanislav Dashevskiy from Forescout Technologies \(en\)](#)

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](#).

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