



# WWBN AVideo has CSRF in configurationUpdate.json.php Enables Full Site Configuration Takeover Including Encoder URL and SMTP Credentials

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

## Summary

<b>CVE</b>	CVE-2026-40925
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 21:16:45 UTC
<b>Updated</b>	2026-04-21 21:16:45 UTC
<b>Description</b>	WWBN AVideo is an open source video platform. In versions 29.0 and prior, `objects/configurationUpdate.json.php` (also r

## Risk And Classification

**Primary CVSS:** v3.1 8.3 HIGH from security-advisories@github.com

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

**Problem Types:** CWE-352 | CWE-352 CWE-352: Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L
3.1	CNA	DECLARED	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Low

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WWBN	AVideo	affected <= 29.0	Not specified

### References

Reference	Source	Link
github.com/WWBN/AVideo/security/advisories/GHSA-vvfw-4m39-fjqf	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/WWBN/AVideo/commit/f9492f5e6123dff0292d5bb3164fde7665dc36b4	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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](https://cve.report/api)

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