



# AVideo: Missing CSRF Protection on State-Changing JSON Endpoints Enables Forced Comment Creation, Vote Manipulation, and Category Asset Deletion

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

## Summary

<b>CVE</b>	CVE-2026-40928
<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 23:16:20 UTC
<b>Updated</b>	2026-04-22 14:17:03 UTC
<b>Description</b>	WWBN AVideo is an open source video platform. In versions 29.0 and prior, multiple AVideo JSON endpoints under `objec

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from security-advisories@github.com

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/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	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**Required**

Scope

**Unchanged**

Confidentiality

**None**

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/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-x2pw-9c38-cp2j	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="#">github.co</a>
github.com/WWBN/AVideo/commit/7aaad601bd9cd7b993ba0ee1b1bea6c32ee7b77c	security-advisories@github.com	<a href="#">github.co</a>
CVE Program record	CVE.ORG	<a href="#">www.cve</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.g</a>

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](#)

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