



AVideo: Arbitrary Stripe Subscription Cancellation via Debug Endpoint and retrieveSubscriptions() Bug

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

Summary

CVE	CVE-2026-34737
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 21:16:32 UTC
Updated	2026-04-01 18:45:32 UTC
Description	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the StripeYPT plugin includes a test.php debug endpoint that allows an attacker to cancel any Stripe subscription via a REST API call. This endpoint is accessible via a REST API call to the debug endpoint. This endpoint is accessible via a REST API call to the debug endpoint.

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from security-advisories@github.com

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

EPSS: 0.000260000 probability, percentile 0.071390000 (date 2026-04-01)

Problem Types: CWE-862 | CWE-862 CWE-862: Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wwbn	AVideo	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WWBN	AVideo	affected <= 26.0	Not specified

References

Reference	Source	Link	Tags
github.com/WWBN/AVideo/security/advisories/GHSA-38rh-4v39-vfxv	security-advisories@github.com	github.com	Exploit, Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#).

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