



CVE-2022-32768

Published on: Not Yet Published

Last Modified on: 08/24/2022 06:15:00 PM UTC

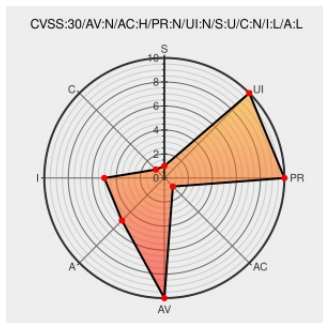
CVE-2022-32768

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [AVideo](#) from [Wwbn](#) contain the following vulnerability:

Multiple authentication bypass vulnerabilities exist in the objects id handling functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request by an authenticated user can lead to unauthorized access and takeover of resources. An attacker can send an HTTP request to trigger this vulnerability. This

vulnerability exists in the Live Schedules plugin, allowing an attacker to bypass authentication by guessing a sequential ID, allowing them to take over the another user's streams.

CVE-2022-32768 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [WWBN](#) - **AVideo** version = **11.6**

Affected Vendor/Software: [WWBN](#) - **AVideo** version = **dev master commit 3f7c0364**

CVSS3 Score: **4.2 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	LOW

CVE References

Description	Tags	Link
TALOS-2022-1536 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1536
AVideo/updateDb.v12.0.sql at e04b1cd7062e16564157a82bae389eedd39fa088 · WWBN/AVideo · GitHub	github.com text/html	CONFIRM github.com/WWBN/AVideo/blob/e04b1cd7062e16564157a82bae389eedd39fa088

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wwbn	Avideo	11.6	All	All	All
cpe:2.3:a:wwbn:avideo:11.6:****:****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-32768 : Multiple authentication bypass vulnerabilities exist in the objects id handling functionality of W... twitter.com/i/web/status/1...	2022-08-22 18:45:59
 /r/netcve	CVE-2022-32768	2022-08-22 19:38:36

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)