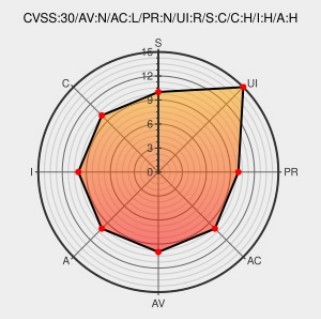
# CVE-2022-32772

Published on: Not Yet Published

Last Modified on: 08/24/2022 02:49:00 PM UTC

## CVE-2022-32772

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Avideo from Wwbn contain the following vulnerability:

A cross-site scripting (xss) vulnerability exists in the footer alerts functionality of WWBN AVideo 11.6 and dev master commit 3f7c0364. A specially-crafted HTTP request can lead to arbitrary Javascript execution. An attacker can get an authenticated user to send a crafted HTTP request to trigger this vulnerability.This vulnerability arrises from the "msg" parameter which is inserted into the document with insufficient sanitization.

CVE-2022-32772 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: 6.1 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| CHANGED | LOW | LOW | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| AVideo/updateDb.v12.0.sql at e04b1cd7062e16564157a82bae389eedd39fa088 · WWBN/AVideo · GitHub | github.com text/html | CONFIRM github.com/WWBN/AVideo/blob/e04b1cd7062e16564157a82bae38 |
| TALOS-2022-1538 \|\| Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | talosintelligence.com text/html | MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1 |

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) |
|---|---|---|
| @RedPacketSec | WWBN AVideo cross-site scripting \| CVE-2022-32772 - redpacketsecurity.com/wwbn-avideo-cr… #CVE #Vulnerability #OSINT #ThreatIntel #Cyber | 2022-08-17 09:02:20 |
| @CVEreport | CVE-2022-32772 : A cross-site scripting xss vulnerability exists in the footer alerts functionality of WWBN AVide… twitter.com/i/web/status/1… | 2022-08-22 18:47:45 |
| /r/netcve | CVE-2022-32772 | 2022-08-22 19:38:40 |

← Previous ID

Next ID→