



CVE-2022-26842

Published on: Not Yet Published

Last Modified on: 08/23/2022 07:52:00 PM UTC

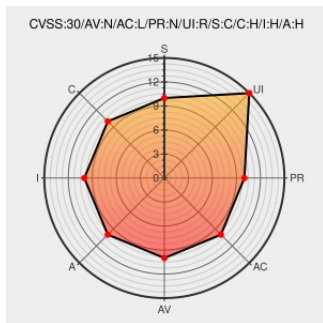
CVE-2022-26842

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

A reflected cross-site scripting (xss) vulnerability exists in the charts tab selection 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.

CVE-2022-26842 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

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

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

CVSS3 Score: **9.6 - CRITICAL**

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

CVE References

Description	Tags	Link
TALOS-2022-1537 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2022-1537
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,

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------