huntr

Bootstrap Tables XSS vulnerability with Table Export plug-in when exportOptions: htmlContent is true in wenzhixin/bootstrap-table

0

✓ Valid Reported on Apr 7th 2022

Description

Hello and thank you for the wonderful library! We use it extensively in our app. However, I think we've identified an XSS vulnerability in the Export plug-in.
If you set the exportOptions in your Bootstrap Table to `true` , then you can force arbitrary Javascript to execute (see the attached PoC). The problem is actually in the jQuery Table Export plug-in, and I've reported it to them as well. But I figure you might also want to fix it here, just in case.
I think the problem can be worked-around by using a corrected onCellHtmlData callback method - which it looks like the library is already attempting to do. However, as evidenced by the vuln, I think for some reason that callback isn't getting executed, and the default onCellHtmlData callback is firing instead, and that default implementation does appear to be vulnerable.

Proof of Concept

https://live.bootstrap-table.com/code/uberbrady/11033

Impact

Disclosing session cookies, disclosing secure session data, exfiltrating data to third-parties.

Occurrences

JS bootstrap-table-export.js L27

I suspect that this line isn't creating an element whose value is the enclos perhaps tree-shaking is removing the function? Or maybe 'uglification' is r element? Either way, this method doesn't seem to be firing. In my own code, when I pass along the onCellHtmlData callback with this function, it does seem to negate the XSS vulnerability.

References

- This is the huntr.dev report for our own application where the vulnerability was reported with us

CVE
CVE-2022-1726
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (6.8)

Registry
Other

Affected Version
1.19.1

Visibility
Public

Status
Fixed

Found by

Brady Wetherington
@uberbrady
maintainer

Fixed by

文翼
@wenzhixin
unranked

Chat with us

This report was seen 631 times.

We are processing your report and will contact the **wenzhixin/bootstrap-table** team within 24 hours. 8 months ago

We have contacted a member of the **wenzhixin/bootstrap-table** team and are waiting to hear back 8 months ago

We have sent a follow up to the **wenzhixin/bootstrap-table** team. We will try again in 7 days. 8 months ago

We have sent a second follow up to the **wenzhixin/bootstrap-table** team. We will try again in 10 days. 7 months ago

We have sent a third and final follow up to the **wenzhixin/bootstrap-table** team. This report is now considered stale. 7 months ago

文翼 validated this vulnerability 6 months ago

Brady Wetherington has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

文翼 marked this as fixed in **1.20.2** with commit **b4a1e5** 6 months ago

文翼 has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

bootstrap-table-export.js#L27 has been validated ✓

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us