



# CVE-2021-42863

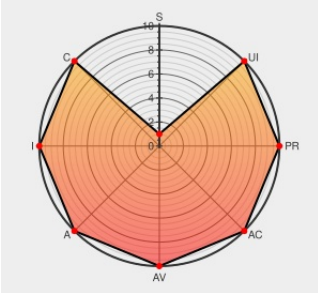
Published on: Not Yet Published

Last Modified on: 05/23/2022 02:23:00 PM UTC

## CVE-2021-42863

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

A buffer overflow in `ecma_builtin_typedarray_prototype_filter()` in JerryScript version `fe3a5c0` allows an attacker to construct a fake object or a fake arraybuffer with unlimited size.

CVE-2021-42863 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                                                            | Tags                                                    | Link                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------|
| Force value conversion in case of TypedArray filter method by galpeter · Pull Request #4794 · jerryscript-project/jerryscript · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/jerryscript-project/jerryscript/pull/4794</a>   |
| Buffer-overflow in ecma-builtin-typedarray-prototype.c · Issue #4793 · jerryscript-project/jerryscript · GitHub                        | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">MISC github.com/jerryscript-project/jerryscript/issues/4793</a> |

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](mailto: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                                  | <a href="#">Jerryscript</a> | <a href="#">Jerryscript</a> | All     | All    | All     | All      |
| cpe:2.3:a:jerryscript:jerryscript:*:*:*:*:*: |                             |                             |         |        |         |          |

No vendor comments have been submitted for this CVE

Social Mentions

| Source                                                                                          | Title                                                                                                                                                                                                                   | Posted (UTC)        |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport     | CVE-2021-42863 : A buffer overflow in ecma_builtin_typedarray_prototype_filter in JerryScript version fe3a5c0 all... <a href="https://twitter.com/i/web/status/1400000000000000000">twitter.com/i/web/status/1...</a>   | 2022-05-12 13:03:57 |
|  @Robo_Alerts | Potentially Critical CVE Detected! CVE-2021-42863 A buffer overflow in ecma_builtin_typedarray_prototype_filter() i... <a href="https://twitter.com/i/web/status/1400000000000000000">twitter.com/i/web/status/1...</a> | 2022-05-12 13:56:01 |
|  /r/netcve    | <a href="#">CVE-2021-42863</a>                                                                                                                                                                                          | 2022-05-12 15:02:34 |

[← Previous ID](#)

[Next ID→](#)