



CVE-2020-13649

Published on: 05/28/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-13649

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

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

parser/js/js-scanner.c in JerryScript 2.2.0 mishandles errors during certain out-of-memory conditions, as demonstrated by a scanner_reverse_info_list NULL pointer dereference and a scanner_scan_all assertion failure.

CVE-2020-13649 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Assertion 'context_p->error == PARSER_ERR_NO_ERROR' failed at jerry-core/parser/js/js-scanner.c(scanner_scan_all):3196 · Issue #3788 · jerryscript-project/jerryscript ·	Third Party Advisory github.com text/html	MISC github.com/jerryscript-project/jerryscript/issues/3788

GitHub

Fix error handling in scanner when in case of OOM (#3793) · jerryscript-project/jerryscript@69f8e78 · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/jerryscript-project/jerryscript/commit/69f8e78c2f8d562bd6d8002b5488f1662ac30d24

NULL dereference in scanner_reverse_info_list · Issue #3786 · jerryscript-project/jerryscript · GitHub

Third Party Advisory

github.com

text/html

MISC

github.com/jerryscript-project/jerryscript/issues/3786

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.

Related QID Numbers

180661 Debian Security Update for iotjs (CVE-2020-13649)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	JerryScript	JerryScript	2.2.0	All	All	All
Application	JerryScript	JerryScript	2.2.0	All	All	All

cpe:2.3:a:jerryscript:jerryscript:2.2.0:*:*:*:*:*:

cpe:2.3:a:jerryscript:jerryscript:2.2.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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](#)