



CVE-2019-1010176

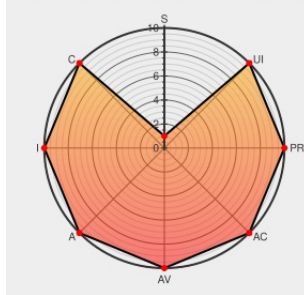
Published on: 07/25/2019 12:00:00 AM UTC

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

CVE-2019-1010176

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

CVSS:30/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:

JerryScript commit 4e58ccf68070671e1fff5cd6673f0c1d5b80b166 is affected by: Buffer Overflow. The impact is: denial of service and possibly arbitrary code execution. The component is: function lit_char_to_utf8_bytes (jerry-core/lit/lit-char-helpers.c:377). The attack vector is: executing crafted javascript code. The fixed version is: after commit 505dace719aebb3308a3af223cfaa985159efae0.

CVE-2019-1010176 has been assigned by [GSD](#) cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [GSD](#) **JerryScript** - JerryScript version **commit 4e58ccf68070671e1fff5cd6673f0c1d5b80b166 [fixed: after commit 505dace719aebb3308a3af223cfaa985159efae0] (as of 2018-09-14)**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description

Heap buffer overflow in lit_char_to_utf8_bytes · Issue #2476 · jerryscript-project/jerryscript · GitHub

Tags

Exploit

Patch

Third Party Advisory

github.com

text/html

Link

MISC

github.com/jerryscript-project/jerryscript/issues/2476

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	Jerryscript	Jerryscript	All	All	All	All
Application	Jerryscript	Jerryscript	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →