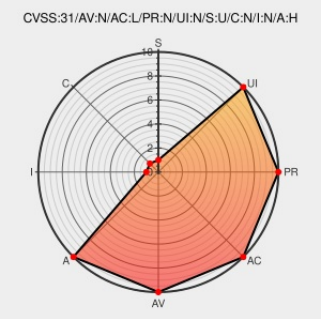
CVE-2017-9250

Published on: 05/28/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:57 PM UTC

CVE-2017-9250

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jerryscript from Jerryscript contain the following vulnerability:

The lexer_process_char_literal function in jerry-core/parser/js/js-lexer.c in JerryScript 1.0 does not skip memory allocation for empty strings, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via malformed JavaScript source code, related to the jmem_heap_free_block function.

CVE-2017-9250 has been assigned by 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
Do not allocate memory for zero length strings. (#1844) · jerryscript-project/jerryscript@e58f288	Patch Third Party Advisory github.com	CONFIRM github.com/jerryscript-project/jerryscript/commit/e58f2880df608652aff7fd35c45b242467ec0e79

project/jerryscript@e581288 · GitHub	text/html	
Denial of Service: Null Pointer De-reference · Issue #1821 · jerryscript-project/jerryscript · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/jerryscript-project/jerryscript/issues/1821
Do not allocate memory for zero length strings. · zherczeg/jerryscript@03a8c63 · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/zherczeg/jerryscript/commit/03a8c630f015f63268639d3ed3bf82cff6fa7
F5 BIG-IP Bug in Web Configuration Utility, iControl REST, and iControl SOAP Lets Remote Users Delete Arbitrary Files on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1038413

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	1.0	-	All	All
Application	Jerryscript	Jerryscript	1.0	-	All	All

cpe:2.3:a:jerryscript:jerryscript:1.0:-:*:*:*:*:*:*:

cpe:2.3:a:jerryscript:jerryscript:1.0:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→