

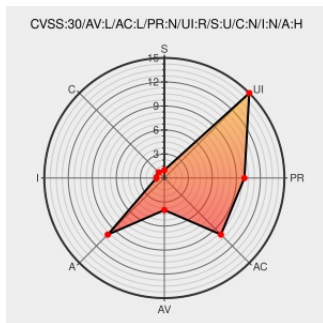


CVE-2018-11590

Published on: 05/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11590

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

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

Espruino before 1.99 allows attackers to cause a denial of service (application crash) with a user crafted input file via an integer overflow during syntax parsing. This was addressed by fixing stack size detection on Linux in jsutils.c.

CVE-2018-11590 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
	Exploit Vendor Advisory github.com application/octet-stream	MISC github.com/espruino/Espruino/files/2019243/so_0.txt

stack over flow error during parsing · Issue #1427 · espruino/Espruino · GitHub

Issue Tracking

Vendor Advisory

github.com

text/html

MISC github.com/espruino/Espruino/issues/1427

Fix stack size detection on Linux (fix #1427) · espruino/Espruino@a0d7f43 · GitHub

Patch

Vendor Advisory

github.com

text/html

MISC github.com/espruino/Espruino/commit/a0d7f432abee692402c00e8b615ff5982dde978

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
Operating System	Espruino	Espruino	All	All	All	All
Operating System	Espruino	Espruino	All	All	All	All

cpe:2.3:o:espruino:espruino:*.***.***.***:

cpe:2.3:o:espruino:espruino:*.***.***.***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →