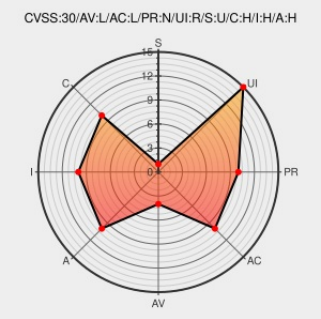
CVE-2018-11595

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

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

CVE-2018-11595

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) and a potential Escalation of Privileges with a user crafted input file via a Buffer Overflow during syntax parsing, because strncat is misused.

CVE-2018-11595 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
multiple stack buffer overflows inside jslex parsing · Issue #1425 · espruino/Espruino · GitHub	Issue Tracking, Vendor Advisory, github.com, text/html	MISC github.com/espruino/Espruino/issues/1425

Fix strncat/cpy bounding issues (fix #1425) · espruino/Espruino@0a76198 · GitHub	Patch Vendor Advisory github.com text/html	MISC github.com/espruino/Espruino/commit/0a7619875bf79877907205f6bee08465b89ff10
	Exploit Vendor Advisory github.com application/octet-stream	MISC github.com/espruino/Espruino/files/2019210/test_0.txt
	Exploit Vendor Advisory github.com application/octet-stream	MISC github.com/espruino/Espruino/files/2019220/test_4.txt
	Exploit Vendor Advisory github.com application/octet-stream	MISC github.com/espruino/Espruino/files/2019216/test_2.txt

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→