



CVE-2022-44318

Published on: Not Yet Published

Last Modified on: 11/08/2022 09:56:00 PM UTC

CVE-2022-44318

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

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

PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StringStrcat function in cstdlib/string.c when called from ExpressionParseFunctionCall.

CVE-2022-44318 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

CVE References

Description	Tags	Link
Multiple Heap Buffer Overflows in PicoC at Various Locations (#48) · Issues · Zik Saleeba / picoc · GitLab	gitlab.com text/html	gitlab.com/zsaleeba/picoc/-/issues/48
Multiple Heap Buffer Overflows in PicoC at Various Locations · Issue #37 · jpoirier/picoc · GitHub	github.com text/html	github.com/jpoirier/picoc/issues/37

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

Proof of concept for CVE-2022-44318

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Picoc Project	Picoc	3.2.2	All	All	All
cpe:2.3:a:picoc_project:picoc:3.2.2:*:*:*:*:*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-44318 : PicoC Version 3.2.2 was discovered to contain a heap buffer overflow in the StringStrcat function... twitter.com/i/web/status/1...	2022-11-08 15:07:20
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-44318 PicoC Version 3.2.2 was discovered to contain a heap buffer overf... twitter.com/i/web/status/1...	2022-11-08 15:56:00
 /r/netcve	CVE-2022-44318	2022-11-08 15:38:47

[← Previous ID](#)[Next ID →](#)