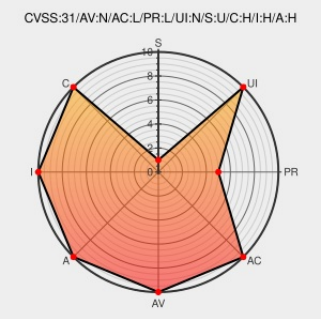
CVE-2021-43083

Published on: Not Yet Published

Last Modified on: 01/04/2022 06:00:00 PM UTC

CVE-2021-43083

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



Certain versions of Plc4x from Apache contain the following vulnerability:

Apache PLC4X - PLC4C (Only the C language implementation was effected) was vulnerable to an unsigned integer underflow flaw inside the tcp transport. Users should update to 0.9.1, which addresses this issue. However, in order to exploit this vulnerability, a user would have to actively connect to a mallicious device which could send a response with invalid content. Currently we consider the probability of this being exploited as quite minimal, however this could change in the future, especially with the industrial networks growing more and more together.

CVE-2021-43083 has been assigned by security@apache.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache PLC4X** version **<= 0.9.0**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
oss-security - CVE-2021-43083: Apache PLC4X 0.9.0 Buffer overflow in PLC4C via crafted server response	www.openwall.com text/html	MLIST [oss-security] 20211220 CVE-2021-43083: Apache PLC4X 0.9.0 Buffer overflow in PLC4C via crafted server response
No Description Provided	lists.apache.org text/html	MISC lists.apache.org/thread/jxx6qc84z60xbbhn6vp2s5qf09psrtc7

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	Apache	Plc4x	All	All	All	All

cpe:2.3:a:apache:plc4x:*:*:*:*:*:*:*:*:

Discovery Credit

Apache PLC4X would like to thank Eugene Lim for reporting this issue.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43083 : #Apache PLC4X - PLC4C Only the C language implementation was effected was vulnerable to an unsig… twitter.com/i/web/status/1…	2021-12-19 08:29:32
/r/netcve	CVE-2021-43083	2021-12-19 09:38:23

← Previous ID

Next ID→