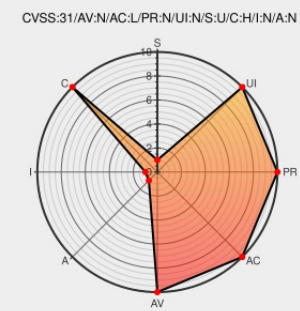
CVE-2023-35849

Published on: Not Yet Published

Last Modified on: 06/26/2023 05:57:00 PM UTC

CVE-2023-35849

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



Certain versions of Picotcp from Virtualsquare contain the following vulnerability:

VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 does not properly check whether header sizes would result in accessing data outside of a packet.

CVE-2023-35849 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	HIGH	NONE	NONE

CVE References

Description	Tags	Link
More checks for correct header sizes · virtualsquare/picotcp@4b9a167 · GitHub	github.com text/html	MISC github.com/virtualsquare/picotcp/commit/4b9a16764f2b12b611de9c34a50b4713d10ca401

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Virtualsquare	Picotcp	All	All	All	All

cpe:2.3:a:virtualsquare:picotcp:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-35849 : VirtualSquare picoTCP aka PicoTCP-NG through 2.1 does not properly check whether header sizes wo… twitter.com/i/web/status/1…	2023-06-19 03:05:09

← Previous ID

Next ID→