



# CVE-2020-17445

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-17445
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-11 23:15:00 UTC
<b>Updated</b>	2020-12-14 21:55:00 UTC
<b>Description</b>	An issue was discovered in picoTCP 1.7.0. The code for processing the IPv6 destination options does not check for a valid

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Altran</a>	<a href="#">Picotcp</a>	All	All	All	All

## References

Reference	Source	Link	Tags
VU#815128 - Embedded TCP/IP stacks have memory corruption vulnerabilities	MISC	<a href="http://www.kb.cert.org">www.kb.cert.org</a>	Third Party Advisory, US Gov
Multiple Embedded TCP/IP Stacks   CISA	MISC	<a href="http://us-cert.cisa.gov">us-cert.cisa.gov</a>	Third Party Advisory, US Gov
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**