CVE-2020-17442

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-17442
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-11 23:15:00 UTC
Updated	2020-12-14 20:08:00 UTC
Description	An issue was discovered in picoTCP 1.7.0. The code for parsing the hop-by-hop IPv6 extension headers does not validate

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

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

References

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

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report