



CVE-2020-14509

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

Summary

CVE	CVE-2020-14509
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-16 20:15:00 UTC
Updated	2021-11-04 18:22:00 UTC
Description	Multiple memory corruption vulnerabilities exist in CodeMeter (All versions prior to 7.10) where the packet parser mechanism

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wibu	Codemeter	All	All	All	All
Application	Wibu	Codemeter	All	All	All	All

References

Reference	Source	Link	Tags
Wibu-Systems CodeMeter (Update A) CISA	MISC	us-cert.cisa.gov	Third Party Advisory, US Government Resource
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.

Legacy QID Mappings

- [590727](#) WIBU CodeMeter PASVisu Multiple Vulnerabilities
- [590734](#) WIBU Codemeter Runtime PAS4000 Multiple Vulnerabilities (adv_1005485-de-02)
- [590802](#) Siemens Remote Connect Client Multiple Vulnerabilities (SSA-455843)
- [590878](#) Schneider Electric Wibu-Systems CodeMeter Multiple Vulnerabilities (SEVD-2020-287-02)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)