



CVE-2021-22663

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

Summary

CVE	CVE-2021-22663
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-09 17:15:00 UTC
Updated	2021-05-03 16:49:00 UTC
Description	Cscape (All versions prior to 9.90 SP3.5) lacks proper validation of user-supplied data when parsing project files. This could

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hornerautomation	Cscape	All	All	All	All
Application	Siemens	Cscape	All	All	All	All
Application	Siemens	Cscape	9.90	-	All	All
Application	Siemens	Cscape	9.90	sp1	All	All
Application	Siemens	Cscape	9.90	sp3	All	All
Application	Siemens	Cscape	All	All	All	All
Application	Siemens	Cscape	9.90	-	All	All
Application	Siemens	Cscape	9.90	sp1	All	All
Application	Siemens	Cscape	9.90	sp3	All	All

References

Reference	Source	Link	Tags
Horner Automation Cscape 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.

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

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