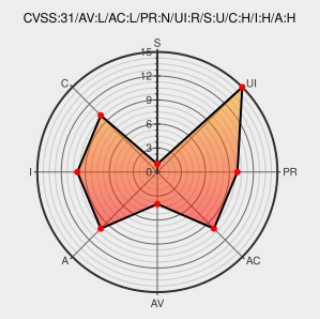
CVE-2021-32995

Published on: 08/25/2021 12:00:00 AM UTC

Last Modified on: 07/02/2022 06:18:00 PM UTC

CVE-2021-32995

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



Certain versions of Cscape from Hornerautomation contain the following vulnerability:

Cscape (All Versions prior to 9.90 SP5) lacks proper validation of user-supplied data when parsing project files. This could lead to an out-of-bounds write. An attacker could leverage this vulnerability to execute code in the context of the current process.

CVE-2021-32995 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Horner Automation Cscape | CISA	us-cert.cisa.gov text/html	MISC us-cert.cisa.gov/ics/advisories/icsa-21-224-02

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

590526 Horner Automation Cscape Multiple Vulnerabilities (ICSA-21-224-02)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hornerautomation	Cscape	All	All	All	All
Application	Hornerautomation	Cscape	9.90	-	All	All
Application	Hornerautomation	Cscape	9.90	sp1	All	All
Application	Hornerautomation	Cscape	9.90	sp2	All	All
Application	Hornerautomation	Cscape	9.90	sp3	All	All
Application	Hornerautomation	Cscape	9.90	sp4	All	All

cpe:2.3:a:hornerautomation:cscape:*:*:*:*:*:*:*:*:

cpe:2.3:a:hornerautomation:cscape:9.90:-:*:*:*:*:*:*:

cpe:2.3:a:hornerautomation:cscape:9.90:sp1:*:*:*:*:*:*:

cpe:2.3:a:hornerautomation:cscape:9.90:sp2:*:*:*:*:*:*:

cpe:2.3:a:hornerautomation:cscape:9.90:sp3:*:*:*:*:*:*:

cpe:2.3:a:hornerautomation:cscape:9.90:sp4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-32995 : Cscape All Versions prior to 9.90 SP5 lacks proper validation of user-supplied data when parsing… twitter.com/i/web/status/1…	2021-08-25 19:17:03
@RemotelyAlerts	Severity: ?? | Cscape (All Versions prior to 9.90 SP5) ... | CVE-2021-32995 | Link for more: alerts.remotelyrmm.com/CVE-2021-32995	2022-07-02 19:28:31

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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