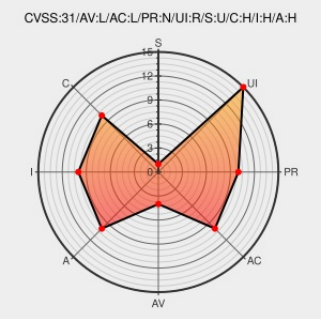
CVE-2021-44462

Published on: Not Yet Published

Last Modified on: 04/04/2022 03:38:00 PM UTC

CVE-2021-44462

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



Certain versions of Cscape Envisionrv from Hornerautomation contain the following vulnerability:

This vulnerability can be exploited by parsing maliciously crafted project files with Horner Automation Cscape EnvisionRV v4.50.3.1 and prior. The issues result from the lack of proper validation of user-supplied data, which can result in reads and writes past the end of allocated data structures. User interaction is required to exploit this vulnerability as an attacker must trick a valid user to open a malicious HMI project file.

CVE-2021-44462 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Horner Automation** - **Cscape EnvisionRV** version **<= v4.50.3.1**

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link

Horner Automation Cscape EnvisionRV | CISA	www.cisa.gov text/html	CONFIRM	www.cisa.gov/uscert/ics/advisories/icsa-21-355-02

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hornerautomation	Cscape Envisionrv	All	All	All	All

cpe:2.3:a:hornerautomation:cscape_envisionrv:*:*:*:*:*:*:*:*:

Discovery Credit

Michael Heinzl reported this vulnerability to CISA.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-44462 : This vulnerability can be exploited by parsing maliciously crafted project files with Horner Autom… twitter.com/i/web/status/1…	2022-03-25 19:18:56
/r/netcve	CVE-2021-44462	2022-03-25 20:38:57

← Previous ID

Next ID→