



# 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 [Cscope Envisionrv](#) from [Hornerautomation](#) contain the following vulnerability:

This vulnerability can be exploited by parsing maliciously crafted project files with Horner Automation Cscope 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](#) - **Cscope EnvisionRV** version <= v4.50.3.1

CVSS3 Score: **7.1 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **5.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>NONE</b>         |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type                                                    | Vendor                           | Product                           | Version | Update | Edition | Language |
|---------------------------------------------------------|----------------------------------|-----------------------------------|---------|--------|---------|----------|
| Application                                             | <a href="#">Hornerautomation</a> | <a href="#">Cscape Envisionrv</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-03-25 19:18:56 |
|  /r/netcve  | <a href="#">CVE-2021-44462</a>                                                                                                                                                                           | 2022-03-25 20:38:57 |

[← Previous ID](#)[Next ID →](#)