



# CVE-2021-22816

Published on: 01/28/2022 12:00:00 AM UTC

Last Modified on: 02/03/2022 01:31:00 PM UTC

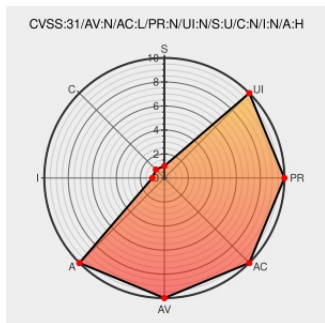
## CVE-2021-22816

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Scadapack 312e](#) from [Schneider-electric](#) contain the following vulnerability:

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause a Denial of Service of the RTU when receiving a specially crafted request over Modbus, and the RTU is configured as a Modbus server. Affected Products: SCADAPack 312E, 313E, 314E, 330E, 333E, 334E, 337E, 350E and 357E RTUs

with firmware V8.18.1 and prior

CVE-2021-22816 has been assigned by [cybersecurity@schneider-electric.com](mailto:cybersecurity@schneider-electric.com) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **7.8 - HIGH**

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

## CVE References

| Description | Tags                                            | Link                                                                                  |
|-------------|-------------------------------------------------|---------------------------------------------------------------------------------------|
|             | <a href="#">download.schneider-electric.com</a> | <a href="#">MISC download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-313-01</a> |

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).

## Related QID Numbers

590896 Schneider Electric SCADAPack 300E Series RTU Vulnerability (SEVD-2021-313-01)

## Known Affected Configurations (CPE V2.3)

| Type                                                                                         | Vendor                             | Product                                 | Version | Update | Edition | Language |
|----------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------|---------|--------|---------|----------|
| Hardware    | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 312e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 312e Firmware</a> | All     | All    | All     | All      |
| Hardware    | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 313e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 313e Firmware</a> | All     | All    | All     | All      |
| Hardware   | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 314e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 314e Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 330e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 330e Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 333e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 333e Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 334e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 334e Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 337e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 337e Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 350e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 350e Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 357e</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Scadapack 357e Firmware</a> | All     | All    | All     | All      |

cpe:2.3:h:schneider-electric:scadapack\_312e:-:\*\*\*\*\*:

|                                                             |
|-------------------------------------------------------------|
| cpe:2.3:o:schneider-electric:scadapack_312e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_313e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_313e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_314e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_314e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_330e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_330e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_333e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_333e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_334e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_334e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_337e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_337e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_350e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_350e_firmware:*****: |
| cpe:2.3:h:schneider-electric:scadapack_357e:-:*****:        |
| cpe:2.3:o:schneider-electric:scadapack_357e_firmware:*****: |

No vendor comments have been submitted for this CVE

| Social Mentions                                                                               |                                                                                                                                                                                                          |                     |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Source                                                                                        | Title                                                                                                                                                                                                    | Posted (UTC)        |
|  @CVEreport | CVE-2021-22816 : A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could ca... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-01-28 20:22:40 |
|  /r/netcve  | <a href="#">CVE-2021-22816</a>                                                                                                                                                                           | 2022-01-28 20:39:09 |

[site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)