



# CVE-2018-11447

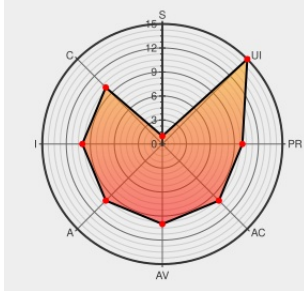
Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:17 PM UTC

## CVE-2018-11447

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Scalance M875](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SCALANCE M875 (All versions). The web interface on port 443/tcp could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link. Successful exploitation requires user interaction by an legitimate user, who must be authenticated to the web interface as

administrative user. A successful attack could allow an attacker to interact with the web interface as an administrative user. This could allow the attacker to read or modify the device configuration, or to exploit other vulnerabilities that require authentication as administrative user. At the time of advisory publication no public exploitation of this security vulnerability was known.

CVE-2018-11447 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [S](#) **Siemens AG - SCALANCE M875** version **SCALANCE M875 All versions**

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</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>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

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

## CVE References

| Description | Tags                                                                                                               | Link                                                                                                                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <a href="#">Third Party Advisory</a><br><a href="#">cert-portal.siemens.com</a><br><a href="#">application/pdf</a> |  <a href="https://cert-portal.siemens.com/productcert/pdf/ssa-977428.pdf">CONFIRM cert-portal.siemens.com/productcert/pdf/ssa-977428.pdf</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

591096 Siemens SCALANCE M875 Multiple Vulnerabilities (SSA-977428)

## Known Affected Configurations (CPE V2.3)

| Type                                                                                        | Vendor                  | Product                                | Version | Update | Edition | Language |
|---------------------------------------------------------------------------------------------|-------------------------|----------------------------------------|---------|--------|---------|----------|
| Hardware   | <a href="#">Siemens</a> | <a href="#">Scalance M875</a>          | -       | All    | All     | All      |
| Hardware  | <a href="#">Siemens</a> | <a href="#">Scalance M875</a>          | -       | All    | All     | All      |
| Operating System                                                                            | <a href="#">Siemens</a> | <a href="#">Scalance M875 Firmware</a> | -       | All    | All     | All      |
| Operating System                                                                            | <a href="#">Siemens</a> | <a href="#">Scalance M875 Firmware</a> | -       | All    | All     | All      |
| cpe:2.3:h:siemens:scalance_m875:-:~::~~::~~::~~::~~::~~::~~:::                              |                         |                                        |         |        |         |          |
| cpe:2.3:h:siemens:scalance_m875:-:~::~~::~~::~~::~~::~~::~~:::                              |                         |                                        |         |        |         |          |
| cpe:2.3:o:siemens:scalance_m875_firmware:-:~::~~::~~::~~::~~::~~::~~:::                     |                         |                                        |         |        |         |          |
| cpe:2.3:o:siemens:scalance_m875_firmware:-:~::~~::~~::~~::~~::~~::~~:::                     |                         |                                        |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

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](#).

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