



# CVE-2019-18330

Published on: 12/12/2019 12:00:00 AM UTC

Last Modified on: 03/04/2022 10:21:00 PM UTC

## CVE-2019-18330

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Sppa-t3000 Ms3000 Migration Server](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SPPA-T3000 MS3000 Migration Server (All versions). An attacker with network access to the MS3000 Server could cause a Denial-of-Service condition and potentially gain remote code execution by sending specifically crafted packets to 5010/tcp. This vulnerability is independent from CVE-2019-18323,

CVE-2019-18324, CVE-2019-18325, CVE-2019-18326, CVE-2019-18327, CVE-2019-18328, and CVE-2019-18329. Please note that an attacker needs to have network access to the MS3000 in order to exploit this vulnerability. At the time of advisory publication no public exploitation of this security vulnerability was known.

CVE-2019-18330 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [S](#) **Siemens** - **SPPA-T3000 MS3000 Migration Server** version **All versions**

CVSS3 Score: **9.8 - CRITICAL**

| 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>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

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

## CVE References

### Description

### Tags

### Link

Mitigation

Vendor Advisory

cert-portal.siemens.com

application/pdf

 [MISC cert-portal.siemens.com/productcert/pdf/ssa-451445.pdf](https://cert-portal.siemens.com/productcert/pdf/ssa-451445.pdf)

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                                                 | Siemens | <a href="#">Sppa-t3000 Ms3000 Migration Server</a> | All     | All    | All     | All      |
| Application                                                 | Siemens | <a href="#">Sppa-t3000 Ms3000 Migration Server</a> | All     | All    | All     | All      |
| cpe:2.3:a:siemens:sppa-t3000_ms3000_migration_server:*****: |         |                                                    |         |        |         |          |
| cpe:2.3:a:siemens:sppa-t3000_ms3000_migration_server:*****: |         |                                                    |         |        |         |          |

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](#)