

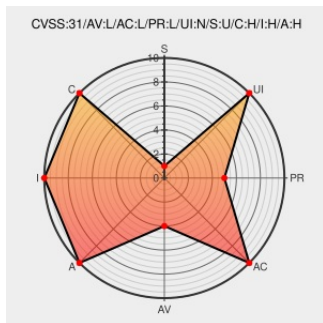


CVE-2019-18297

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

Last Modified on: 03/04/2022 10:16:00 PM UTC

CVE-2019-18297

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

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 local access to the MS3000 Server and low privileges could gain root privileges by sending specifically crafted packets to a named pipe. Please note that an attacker needs to have local 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-2019-18297 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

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

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description

Siemens Security Advisory - SPPA-T3000 Code Execution ≈ Packet Storm

Tags

Third Party Advisory

VDB Entry

packetstormsecurity.com

text/html

Mitigation

Vendor Advisory

cert-portal.siemens.com

application/pdf

Link

📄

 MISC packetstormsecurity.com/files/155665/Siemens-Security-Advisory-SPPA-T3000-Code-Execution.html

🌐

 CONFIRM N/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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Sppa-t3000 Ms3000 Migration Server	All	All	All	All
Application	Siemens	Sppa-t3000 Ms3000 Migration Server	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 →