

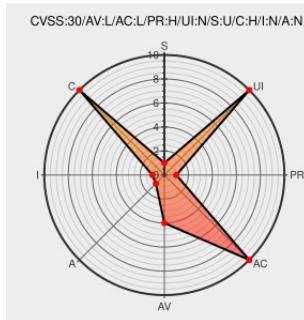


CVE-2017-10606

Published on: 10/13/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:29 PM UTC

CVE-2017-10606

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

Certain versions of [Srx300](#) from [Juniper](#) contain the following vulnerability:

Version 4.40 of the TPM (Trusted Platform Module) firmware on Juniper Networks SRX300 Series has a weakness in generating cryptographic keys that may allow an attacker to decrypt sensitive information in SRX300 Series products. The TPM is used in the SRX300 Series to encrypt sensitive configuration data. While other

products also ship with a TPM, no other products or platforms are affected by this vulnerability. Customers can confirm the version of TPM firmware via the 'show security tpm status' command. This issue was discovered by an external security researcher. No other Juniper Networks products or platforms are affected by this issue.

CVE-2017-10606 has been assigned by [JJ](#) sirt@juniper.net to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [JJ](#) **Juniper Networks - Junos OS** version **15.1X49** prior to **TPM firmware version 4.43**

Vulnerability Patch/Work Around

There is no known workaround for this issue.

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
2017-10 Security Bulletin: SRX Series: Cryptographic weakness in SRX300 Series TPM Firmware (CVE-2017-10606) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	 CONFIRM kb.juniper.net/JSA10809

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
Hardware  	Juniper	Srx300	-	All	All	All
Hardware  	Juniper	Srx300	-	All	All	All
Hardware  	Juniper	Srx320	-	All	All	All
Hardware  	Juniper	Srx320	-	All	All	All
Hardware  	Juniper	Srx340	-	All	All	All
Hardware  	Juniper	Srx340	-	All	All	All
Hardware  	Juniper	Srx345	-	All	All	All
Hardware  	Juniper	Srx345	-	All	All	All
Operating System	Juniper	Trusted Platform Module Firmware	4.40	All	All	All
Operating System	Juniper	Trusted Platform Module Firmware	4.40	All	All	All

```
cpe:2.3:h:juniper:srx300:-:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx300:-:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx320:-:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx320:-:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx340:-:*:*:*:*:*:
```

```
cpe:2.3:h:juniper:srx340:-:*:*:*:*:*:
```

cpe:2.3:h:juniper:srx345:-:*:*:*:*:*:
cpe:2.3:h:juniper:srx345:-:*:*:*:*:*:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*:*:*:*:*:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*:*:*:*:*:

cpe:2.3:h:juniper:srx345:-:*****:
cpe:2.3:h:juniper:srx345:-:*****:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*****:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*****:

cpe:2.3:h:juniper:srx345:-:*:*:*:*:*:
cpe:2.3:h:juniper:srx345:-:*:*:*:*:*:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*:*:*:*:*:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*:*:*:*:*:

cpe:2.3:h:juniper:srx345:-:*:*:*:*:*:
cpe:2.3:h:juniper:srx345:-:*:*:*:*:*:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*:*:*:*:*:
cpe:2.3:o:juniper:trusted_platform_module_firmware:4.40:*:*:*:*:*:

[← 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