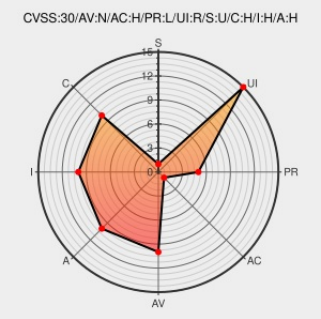
CVE-2017-10623

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

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

CVE-2017-10623

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Junos Space from Juniper contain the following vulnerability:

Lack of authentication and authorization of cluster messages in Juniper Networks Junos Space may allow a man-in-the-middle type of attacker to intercept, inject or disrupt Junos Space cluster operations between two nodes. Affected releases are Juniper Networks Junos Space all versions prior to 17.1R1.

CVE-2017-10623 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Juniper Networks** - **Junos Space** version **versions prior to 17.1R1**

Vulnerability Patch/Work Around

There are no viable workarounds for this issue. It is good security practice to limit the exploitable attack surface of critical infrastructure networking equipment. Use access lists or firewall filters to limit access to the device from trusted, administrative networks or hosts.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
2017-10 Security Bulletin: Junos Space: Multiple vulnerabilities resolved in 17.1R1 release - Juniper Networks	Vendor Advisory kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA10826

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Juniper	Junos Space	All	All	All	All

cpe:2.3:a:juniper:junos_space:*:*:*:*:*:*:*:*:

← Previous ID

Next ID→