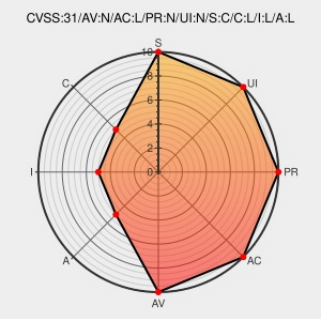
CVE-2020-1675

Published on: 10/16/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 05:35:00 PM UTC

CVE-2020-1675 - advisory for JSA11072

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



Certain versions of Mist Cloud Ui from Juniper contain the following vulnerability:

When Security Assertion Markup Language (SAML) authentication is enabled, Juniper Networks Mist Cloud UI might incorrectly process invalid authentication certificates which could allow a malicious network-based user to access unauthorized data. This issue affects all Juniper Networks Mist Cloud UI versions prior to September 2 2020.

CVE-2020-1675 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Juniper Networks** - **MIST Cloud UI** version **< 09/02/2020**

Vulnerability Patch/Work Around

No workarounds are required since the issue has been resolved in the Mist cloud UI.

CVSS3 Score: 8.3 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	LOW

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
2020-10 Security Bulletin: Mist Cloud User Interface: Multiple vulnerabilities due to SAML authentication. - Juniper Networks	Vendor Advisory kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA11072

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Small Powershell Script to detect Running Printer Spoolers on Domain Controller

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Juniper	Mist Cloud Ui	All	All	All	All
Application	Juniper	Mist Cloud Ui	All	All	All	All

cpe:2.3:a:juniper:mist_cloud_ui:*:*:*:*:*:*:*:*:

cpe:2.3:a:juniper:mist_cloud_ui:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@lonut_Ilascu	They also acknowledged PrintNightmare as a separate vulnerability from CVE-2020-1675 and said it's being exploited… twitter.com/i/web/status/1…	2021-07-02 08:57:59

← Previous ID

Next ID→