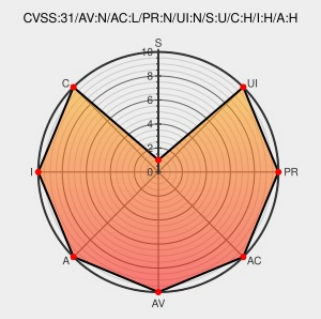
CVE-2021-31349

Published on: 10/19/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 03:32:00 PM UTC

CVE-2021-31349 - advisory for JSA11256

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



Certain versions of 128 Technology Session Smart Router from Juniper contain the following vulnerability:

The usage of an internal HTTP header created an authentication bypass vulnerability (CWE-287), allowing an attacker to view internal files, change settings, manipulate services and execute arbitrary code. This issue affects all Juniper Networks 128 Technology Session Smart Router versions prior to 4.5.11, and all versions of 5.0 up to and including 5.0.1.

CVE-2021-31349 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Juniper Networks** - **128 Technology Session Smart Router** version **< 4.5.11**

Affected Vendor/Software: **Juniper Networks** - **128 Technology Session Smart Router** version **<= 5.0.1**

Vulnerability Patch/Work Around

While no workarounds exist for this vulnerability, risk exposure can be mitigated. HTTP access to the SSR occurs on TCP port 443. It is recommended to install firewall rules to permit access only from trusted IP addresses.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
2021-10 Security Bulletin: Session Smart Router: Authentication Bypass Vulnerability (CVE-2021-31349) - Juniper Networks	kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA11256

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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Juniper	128 Technology Session Smart Router	-	All	All	All
Operating System	Juniper	128 Technology Session Smart Router Firmware	All	All	All	All
Operating System	Juniper	128 Technology Session Smart Router Firmware	All	All	All	All

cpe:2.3:h:juniper:128_technology_session_smart_router:-:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:128_technology_session_smart_router_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:128_technology_session_smart_router_firmware:*:*:*:*:*:*:*:*:

Discovery Credit

128 Technology was notified via the JVN community of the vulnerability as JVN#85073657.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-31349 : The usage of an internal HTTP header created an authentication bypass vulnerability CWE-287 , all… twitter.com/i/web/status/1…	2021-10-19 18:27:14

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report