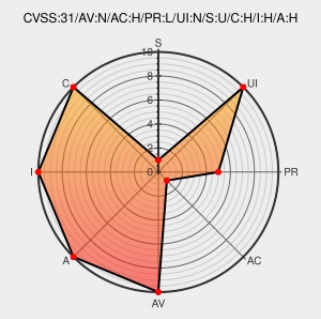
CVE-2021-31350

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

Last Modified on: 10/25/2021 12:58:00 PM UTC

CVE-2021-31350 - advisory for JSA11215

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



Certain versions of Junos from Juniper contain the following vulnerability:

An Improper Privilege Management vulnerability in the gRPC framework, used by the Juniper Extension Toolkit (JET) API on Juniper Networks Junos OS and Junos OS Evolved, allows a network-based, low-privileged authenticated attacker to perform operations as root, leading to complete compromise of the targeted system. The issue is caused by the JET service daemon (jsd) process authenticating the user, then passing configuration operations directly to the management daemon (mgd) process, which runs as root. This issue affects Juniper Networks Junos OS: 18.4 versions prior to 18.4R1-S8, 18.4R2-S8, 18.4R3-S8; 19.1 versions prior to 19.1R2-S3, 19.1R3-S5; 19.2 versions prior to 19.2R1-S7, 19.2R3-S2; 19.3 versions prior to 19.3R2-S6, 19.3R3-S2; 19.4 versions prior to 19.4R1-S4, 19.4R2-S4, 19.4R3-S3; 20.1 versions prior to 20.1R2-S2, 20.1R3; 20.2 versions prior to 20.2R2-S3, 20.2R3; 20.3 versions prior to 20.3R2-S1, 20.3R3; 20.4 versions prior to 20.4R2. This issue does not affect Juniper Networks Junos OS versions prior to 18.4R1. Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-EVO; 21.1-EVO versions prior to 21.1R2-EVO.

CVE-2021-31350 has been assigned by sirt@juniper.net to track the vulnerability - currently rated as HIGH severity.

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.

Vulnerability Patch/Work Around

Use access lists or firewall filters to limit access to the device via gRPC only from trusted hosts and from trusted administrators

CVSS3 Score: 8.8 - HIGH

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

UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
2021-10 Security Bulletin: Junos OS and Junos OS Evolved: Privilege escalation vulnerability in Juniper Extension Toolkit (JET) (CVE-2021-31350) - Juniper Networks	kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA11215

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	18.4	-	All	All
Operating System	Juniper	Junos	18.4	r1	All	All
Operating System	Juniper	Junos	18.4	r1-s1	All	All
Operating System	Juniper	Junos	18.4	r1-s2	All	All
Operating System	Juniper	Junos	18.4	r1-s3	All	All
Operating System	Juniper	Junos	18.4	r1-s4	All	All
Operating System	Juniper	Junos	18.4	r1-s5	All	All
Operating System	Juniper	Junos	18.4	r1-s6	All	All
Operating System	Juniper	Junos	18.4	r1-s7	All	All
Operating System	Juniper	Junos	18.4	r2-s8	All	All

Operating System	Juniper	Junos	18.4	r3-s8	All	All
Operating System	Juniper	Junos	19.1	-	All	All
Operating System	Juniper	Junos	19.1	r1	All	All
Operating System	Juniper	Junos	19.1	r1-s1	All	All
Operating System	Juniper	Junos	19.1	r1-s2	All	All
Operating System	Juniper	Junos	19.1	r1-s3	All	All
Operating System	Juniper	Junos	19.1	r1-s4	All	All
Operating System	Juniper	Junos	19.1	r1-s5	All	All
Operating System	Juniper	Junos	19.1	r1-s6	All	All
Operating System	Juniper	Junos	19.1	r2	All	All
Operating System	Juniper	Junos	19.1	r2-s1	All	All
Operating System	Juniper	Junos	19.1	r2-s2	All	All
Operating System	Juniper	Junos	19.1	r3-s5	All	All
Operating System	Juniper	Junos	19.2	-	All	All
Operating System	Juniper	Junos	19.2	r1	All	All
Operating System	Juniper	Junos	19.2	r1-s1	All	All
Operating System	Juniper	Junos	19.2	r1-s2	All	All
Operating System	Juniper	Junos	19.2	r1-s3	All	All
Operating System	Juniper	Junos	19.2	r1-s4	All	All
Operating System	Juniper	Junos	19.2	r1-s5	All	All
Operating System	Juniper	Junos	19.2	r1-s6	All	All
Operating System	Juniper	Junos	19.2	r3-s2	All	All
Operating System	Juniper	Junos	19.3	-	All	All

Operating System	Juniper	Junos	19.3	r1	All	All
Operating System	Juniper	Junos	19.3	r1-s1	All	All
Operating System	Juniper	Junos	19.3	r2	All	All
Operating System	Juniper	Junos	19.3	r2-s1	All	All
Operating System	Juniper	Junos	19.3	r2-s2	All	All
Operating System	Juniper	Junos	19.3	r2-s3	All	All
Operating System	Juniper	Junos	19.3	r2-s4	All	All
Operating System	Juniper	Junos	19.3	r2-s5	All	All
Operating System	Juniper	Junos	19.3	r3-s2	All	All
Operating System	Juniper	Junos	19.4	r1	All	All
Operating System	Juniper	Junos	19.4	r1-s1	All	All
Operating System	Juniper	Junos	19.4	r1-s2	All	All
Operating System	Juniper	Junos	19.4	r1-s3	All	All
Operating System	Juniper	Junos	19.4	r2-s4	All	All
Operating System	Juniper	Junos	19.4	r3-s3	All	All
Operating System	Juniper	Junos	20.1	r1	All	All
Operating System	Juniper	Junos	20.1	r1-s1	All	All
Operating System	Juniper	Junos	20.1	r1-s2	All	All
Operating System	Juniper	Junos	20.1	r1-s3	All	All
Operating System	Juniper	Junos	20.1	r1-s4	All	All
Operating System	Juniper	Junos	20.1	r2	All	All
Operating System	Juniper	Junos	20.1	r2-s1	All	All
Operating System	Juniper	Junos	20.1	r3	All	All

Operating System	Juniper	Junos	20.2	r1	All	All
Operating System	Juniper	Junos	20.2	r1-s1	All	All
Operating System	Juniper	Junos	20.2	r1-s2	All	All
Operating System	Juniper	Junos	20.2	r1-s3	All	All
Operating System	Juniper	Junos	20.2	r2	All	All
Operating System	Juniper	Junos	20.2	r2-s1	All	All
Operating System	Juniper	Junos	20.2	r2-s2	All	All
Operating System	Juniper	Junos	20.2	r3	All	All
Operating System	Juniper	Junos	20.3	r1	All	All
Operating System	Juniper	Junos	20.3	r1-s1	All	All
Operating System	Juniper	Junos	20.3	r2	All	All
Operating System	Juniper	Junos	20.3	r3	All	All
Operating System	Juniper	Junos	20.4	r1	All	All
Operating System	Juniper	Junos	20.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	18.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	19.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	19.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	19.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	19.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	19.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	19.3	r2	All	All
Operating System	Juniper	Junos Os Evolved	19.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	19.4	r1-s1	All	All

Operating System	Juniper	Junos Os Evolved	20.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.2	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.2	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	All	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1-s1	All	All

cpe:2.3:o:juniper:junos:18.4:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1-s5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1-s6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r1-s7:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r2-s8:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.4:r3-s8:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r1-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r1-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r1-s5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r1-s6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.1:r3-s5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1-s5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r1-s6:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.2:r3-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r2-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r2-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r2-s5:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.3:r3-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r1-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r2-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:19.4:r3-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r1-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r1-s4:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.1:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r1-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r1-s3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.2:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.3:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.3:r3:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:20.4:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:18.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.4:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.1:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.1:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.1:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.1:r2-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.1:r2-s2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.2:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.2:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.2:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.3:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.3:r1-s1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.3:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r1:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:21.1:r1-s1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

@softek_jp	Juniper Networks Junos OS の JET の処理に root 権限を奪われる問題 (CVE-2021-31350) [40241] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2021-10-14 08:30:17
@CVEreport	CVE-2021-31350 : An Improper Privilege Management vulnerability in the gRPC framework, used by the Juniper Extensio… twitter.com/i/web/status/1…	2021-10-19 18:27:26

← Previous ID

Next ID→