



CVE-2023-28982

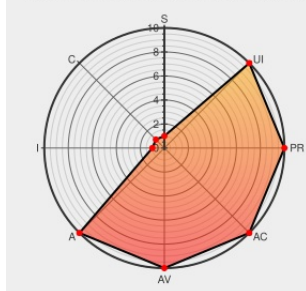
Published on: Not Yet Published

Last Modified on: 05/02/2023 07:07:00 PM UTC

CVE-2023-28982 - advisory for JSA70608

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

A Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS). In a BGP rib sharding scenario, when an attribute of an active BGP route is updated memory will leak. As rpd

memory usage increases over time the rpd process will eventually run out of memory, crash, and restart. The memory utilization can be monitored with the following CLI commands: show task memory show system processes extensive | match rpd This issue affects: Juniper Networks Junos OS 20.3 versions prior to 20.3R3-S2; 20.4 versions prior to 20.4R3-S6; 21.1 versions prior to 21.1R3; 21.2 versions prior to 21.2R3; 21.3 versions prior to 21.3R2. Juniper Networks Junos OS Evolved 20.3-EVO version 20.3R1-EVO and later versions; 20.4-EVO versions prior to 20.4R3-S6-EVO; 21.2-EVO versions prior to 21.2R3-EVO; 21.3-EVO versions prior to 21.3R2-EVO.

CVE-2023-28982 has been assigned by [J SIRT](#) 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

There are no known workarounds for this issue.

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
CEC Juniper Community	supportportal.juniper.net text/html	 CONFIRM supportportal.juniper.net/JSA70608

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.

Related QID Numbers

[44012](#) Juniper Network Operating System (Junos OS) Denial of Service (DoS) Vulnerability (JSA70608)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Juniper	Junos	20.3	-	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	r1-s2	All	All
Operating System	Juniper	Junos	20.3	r2	All	All
Operating System	Juniper	Junos	20.3	r2-s1	All	All
Operating System	Juniper	Junos	20.3	r3	All	All
Operating System	Juniper	Junos	20.3	r3-s1	All	All
Operating System	Juniper	Junos	20.4	-	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	20.4	r2	All	All
Operating System	Juniper	Junos	20.4	r2-s1	All	All
Operating System	Juniper	Junos	20.4	r2-s2	All	All
Operating System	Juniper	Junos	20.4	r3	All	All

System							
Operating System	Juniper	Junos	20.4	r3-s1	All	All	
Operating System	Juniper	Junos	20.4	r3-s2	All	All	
Operating System	Juniper	Junos	20.4	r3-s3	All	All	
Operating System	Juniper	Junos	20.4	r3-s4	All	All	
Operating System	Juniper	Junos	20.4	r3-s5	All	All	
Operating System	Juniper	Junos	21.1	-	All	All	
Operating System	Juniper	Junos	21.1	r1	All	All	
Operating System	Juniper	Junos	21.1	r1-s1	All	All	
Operating System	Juniper	Junos	21.1	r2	All	All	
Operating System	Juniper	Junos	21.1	r2-s1	All	All	
Operating System	Juniper	Junos	21.1	r2-s2	All	All	
Operating System	Juniper	Junos	21.2	-	All	All	
Operating System	Juniper	Junos	21.2	r1	All	All	
Operating System	Juniper	Junos	21.2	r1-s1	All	All	
Operating System	Juniper	Junos	21.2	r1-s2	All	All	
Operating System	Juniper	Junos	21.2	r2	All	All	
Operating System	Juniper	Junos	21.2	r2-s1	All	All	
Operating System	Juniper	Junos	21.2	r2-s2	All	All	
Operating System	Juniper	Junos	21.3	-	All	All	
Operating System	Juniper	Junos	21.3	r1	All	All	
Operating System	Juniper	Junos	21.3	r1-s1	All	All	
Operating System	Juniper	Junos	21.3	r1-s2	All	All	
Operating System	Juniper	Junos Os Evolved	20.3	r1	All	All	

System						
Operating System	Juniper	Junos Os Evolved	20.3	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r1-s3	All	All
Operating System	Juniper	Junos Os Evolved	20.3	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	-	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r2-s3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s4	All	All
Operating System	Juniper	Junos Os Evolved	20.4	r3-s5	All	All
Operating System	Juniper	Junos Os Evolved	21.2	-	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r1-s2	All	All
Operating	Juniper	Junos Os Evolved	21.2	r2	All	All

System						
Operating System	Juniper	Junos Os Evolved	21.2	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	-	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r1-s1	All	All
	cpe:2.3:o:juniper:junos:20.3:-:*:*:*:*:*:					
	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:r1-s2:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.3:r2:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.3:r2-s1:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.3:r3:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.3:r3-s1:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:-:*:*:*:*:*:					
	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:20.4:r2:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r2-s1:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r2-s2:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r3:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r3-s1:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r3-s2:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r3-s3:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r3-s4:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:20.4:r3-s5:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:21.1:-:*:*:*:*:*:					
	cpe:2.3:o:juniper:junos:21.1:r1:*:*:*:*:*:					

cpe:2.3:o:juniper:junos:21.1:r1-s1:*****:
cpe:2.3:o:juniper:junos:21.1:r2:*****:
cpe:2.3:o:juniper:junos:21.1:r2-s1:*****:
cpe:2.3:o:juniper:junos:21.1:r2-s2:*****:
cpe:2.3:o:juniper:junos:21.2:-:*****:
cpe:2.3:o:juniper:junos:21.2:r1:*****:
cpe:2.3:o:juniper:junos:21.2:r1-s1:*****:
cpe:2.3:o:juniper:junos:21.2:r1-s2:*****:
cpe:2.3:o:juniper:junos:21.2:r2:*****:
cpe:2.3:o:juniper:junos:21.2:r2-s1:*****:
cpe:2.3:o:juniper:junos:21.2:r2-s2:*****:
cpe:2.3:o:juniper:junos:21.3:-:*****:
cpe:2.3:o:juniper:junos:21.3:r1:*****:
cpe:2.3:o:juniper:junos:21.3:r1-s1:*****:
cpe:2.3:o:juniper:junos:21.3:r1-s2:*****:
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:r1-s2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.3:r1-s3:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.3:r2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:-:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r1-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r1-s2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r2-s3:*****:

cpe:2.3:o:juniper:junos_os_evolved:20.4:r3:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s2:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s3:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s4:*****:
cpe:2.3:o:juniper:junos_os_evolved:20.4:r3-s5:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:-:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:r1:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:r1-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:r1-s2:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:r2:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:r2-s1:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.2:r2-s2:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.3:-:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.3:r1:*****:
cpe:2.3:o:juniper:junos_os_evolved:21.3:r1-s1:*****:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @RedPacketSec	Juniper Networks Junos OS and Junos OS Evolved denial of service CVE-2023-28982 - redpacketsecurity.com/juniper-network... #CVE... twitter.com/i/web/status/1...	2023-04-13 09:05:44
 @CVEreport	CVE-2023-28982 : A Missing Release of Memory after Effective Lifetime vulnerability in the routing protocol daemon... twitter.com/i/web/status/1...	2023-04-17 21:27:03

[← Previous ID](#)

[Next ID→](#)

