



CVE-2023-28967

Published on: Not Yet Published

Last Modified on: 04/27/2023 06:37:00 PM UTC

CVE-2023-28967 - advisory for JSA70591

[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 Use of Uninitialized Resource vulnerability in the Border Gateway Protocol (BGP) software of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to send specific genuine BGP packets to a device configured with BGP to cause a Denial of Service (DoS) by crashing the Routing Protocol

Daemon (rpd). This issue is triggered when the packets attempt to initiate a BGP connection before a BGP session is successfully established. Continued receipt of these specific BGP packets will cause a sustained Denial of Service condition. This issue is triggerable in both iBGP and eBGP deployments. This issue affects: Juniper Networks Junos OS 21.1 version 21.1R1 and later versions prior to 21.1R3-S5; 21.2 version 21.2R1 and later versions prior to 21.2R3-S2; 21.3 version 21.3R1 and later versions prior to 21.3R3-S2; 21.4 versions prior to 21.4R3; 22.1 versions prior to 22.1R3; 22.2 versions prior to 22.2R2. This issue does not affect Juniper Networks Junos OS versions prior to 21.1R1. This issue affects: Juniper Networks Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions prior to 21.4R3-EVO; 22.1-EVO versions prior to 22.1R3-EVO; 22.2-EVO versions prior to 22.2R2-EVO. This issue does not affect Juniper Networks Junos OS Evolved versions prior to 21.1R1-EVO.

CVE-2023-28967 has been assigned by [J](#) 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

There are no known workarounds for this issue. To reduce the risk of exploitation utilize common security BCPs to limit the exploitable surface by disallowing access to all BGP services on networks and devices to only trusted systems, administrators, networks and hosts.

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/JSA70591

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

44013 Juniper Network Operating System (Junos OS) Denial of Service (DoS) Vulnerability (JSA70591)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	21.1	r3	All	All
Operating System	Juniper	Junos	21.1	r3-s1	All	All
Operating System	Juniper	Junos	21.1	r3-s2	All	All
Operating System	Juniper	Junos	21.1	r3-s3	All	All
Operating System	Juniper	Junos	21.1	r3-s4	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	21.2	r3	All	All
Operating System	Juniper	Junos	21.2	r3-s1	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	21.3	r2	All	All
Operating System	Juniper	Junos	21.3	r2-s1	All	All
Operating System	Juniper	Junos	21.3	r2-s2	All	All
Operating System	Juniper	Junos	21.3	r3	All	All
Operating System	Juniper	Junos	21.3	r3-s1	All	All
Operating System	Juniper	Junos	21.4	-	All	All
Operating System	Juniper	Junos	21.4	r1	All	All
Operating System	Juniper	Junos	21.4	r1-s1	All	All
Operating System	Juniper	Junos	21.4	r1-s2	All	All
Operating System	Juniper	Junos	21.4	r2	All	All
Operating System	Juniper	Junos	21.4	r2-s1	All	All

Operating System	Juniper	Junos	21.4	r2-s2	All	All
Operating System	Juniper	Junos	22.1	r1	All	All
Operating System	Juniper	Junos	22.1	r1-s1	All	All
Operating System	Juniper	Junos	22.1	r1-s2	All	All
Operating System	Juniper	Junos	22.1	r2	All	All
Operating System	Juniper	Junos	22.1	r2-s1	All	All
Operating System	Juniper	Junos	22.1	r2-s2	All	All
Operating System	Juniper	Junos	22.2	r1	All	All
Operating System	Juniper	Junos	22.2	r1-s1	All	All
Operating System	Juniper	Junos	22.2	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	-	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.1	r3-s3	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 System	Juniper	Junos Os Evolved	21.2	r2	All	All

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	21.2	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3-s4	All	All
Operating System	Juniper	Junos Os Evolved	21.2	r3-s5	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
Operating System	Juniper	Junos Os Evolved	21.3	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s2	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s3	All	All
Operating System	Juniper	Junos Os Evolved	21.3	r3-s4	All	All
Operating System	Juniper	Junos Os Evolved	21.4	-	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r1-s2	All	All

Operating System	Juniper	Junos Os Evolved	21.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	21.4	r2-s2	All	All
Operating System	Juniper	Junos Os Evolved	22.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	22.1	r1-s1	All	All
Operating System	Juniper	Junos Os Evolved	22.1	r1-s2	All	All
Operating System	Juniper	Junos Os Evolved	22.1	r2	All	All
Operating System	Juniper	Junos Os Evolved	22.1	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	22.2	r1	All	All
Operating System	Juniper	Junos Os Evolved	22.2	r1-s1	All	All
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:21.1:r3:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:21.1:r3-s1:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:21.1:r3-s2:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:21.1:r3-s3:*:*:*:*:*:						
cpe:2.3:o:juniper:junos:21.1:r3-s4:*:*:*:*:*:						
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:21.2:r3:*****:
cpe:2.3:o:juniper:junos:21.2:r3-s1:*****:
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:21.3:r2:*****:
cpe:2.3:o:juniper:junos:21.3:r2-s1:*****:
cpe:2.3:o:juniper:junos:21.3:r2-s2:*****:
cpe:2.3:o:juniper:junos:21.3:r3:*****:
cpe:2.3:o:juniper:junos:21.3:r3-s1:*****:
cpe:2.3:o:juniper:junos:21.4:-:*****:
cpe:2.3:o:juniper:junos:21.4:r1:*****:
cpe:2.3:o:juniper:junos:21.4:r1-s1:*****:
cpe:2.3:o:juniper:junos:21.4:r1-s2:*****:
cpe:2.3:o:juniper:junos:21.4:r2:*****:
cpe:2.3:o:juniper:junos:21.4:r2-s1:*****:
cpe:2.3:o:juniper:junos:21.4:r2-s2:*****:
cpe:2.3:o:juniper:junos:22.1:r1:*****:
cpe:2.3:o:juniper:junos:22.1:r1-s1:*****:
cpe:2.3:o:juniper:junos:22.1:r1-s2:*****:
cpe:2.3:o:juniper:junos:22.1:r2:*****:
cpe:2.3:o:juniper:junos:22.1:r2-s1:*****:
cpe:2.3:o:juniper:junos:22.1:r2-s2:*****:
cpe:2.3:o:juniper:junos:22.2:r1:*****:
cpe:2.3:o:juniper:junos:22.2:r1-s1:*****:
cpe:2.3:o:juniper:junos:22.2:r1-s2:*****:

cpe:2.3:o:juniper:junos.22.2.r1-s2.*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:-:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:r1:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:r1-s1:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:r2:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:r3:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:r3-s1:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:r3-s2:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.1:r3-s3:*.*.*.*.*
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:21.2:r3:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.2:r3-s1:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.2:r3-s2:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.2:r3-s3:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.2:r3-s4:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.2:r3-s5:*.*.*.*.*
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:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.3:r2:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.3:r2-s1:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.3:r2-s2:*.*.*.*.*
cpe:2.3:o:juniper:junos_os_evolved:21.3:r3:*.*.*.*.*

cpe:2.3:o:juniper:junos_os_evolved:21.3:r3-s1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.3:r3-s2:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.3:r3-s3:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.3:r3-s4:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.4:-:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.4:r1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.4:r1-s1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.4:r1-s2:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.4:r2:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.4:r2-s1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:21.4:r2-s2:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:22.1:r1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:22.1:r1-s1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:22.1:r1-s2:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:22.1:r2:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:22.1:r2-s1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:22.2:r1:****.*.*:
cpe:2.3:o:juniper:junos_os_evolved:22.2: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-2023-28967 - redpacketsecurity.com/juniper-networ... #CVE... twitter.com/i/web/status/1...	2023-04-13 09:05:38
 @CVEreport	CVE-2023-28967 : A Use of Uninitialized Resource vulnerability in the Border Gateway Protocol BGP software of Jun... twitter.com/i/web/status/1...	2023-04-17 21:22:31

[← Previous ID](#)

Next ID→

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)