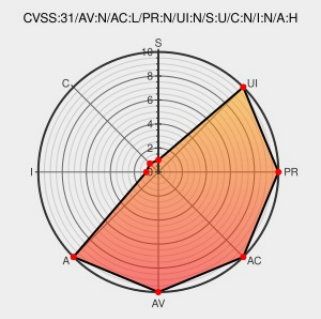
CVE-2020-1648

Published on: 07/17/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 05:34:00 PM UTC

CVE-2020-1648 - advisory for JSA11035

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



Certain versions of Junos from Juniper contain the following vulnerability:

On Juniper Networks Junos OS and Junos OS Evolved devices, processing a specific BGP packet can lead to a routing process daemon (RPD) crash and restart. This issue can occur even before the BGP session with the peer is established. Repeated receipt of this specific BGP packet can result in an extended Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 18.2X75 versions starting from 18.2X75-D50.8, 18.2X75-D60 and later versions, prior to 18.2X75-D52.8, 18.2X75-D53, 18.2X75-D60.2, 18.2X75-D65.1, 18.2X75-D70; 19.4 versions 19.4R1 and 19.4R1-S1; 20.1 versions prior to 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved: 19.4-EVO versions prior to 19.4R2-S2-EVO; 20.1-EVO versions prior to 20.1R2-EVO. This issue does not affect: Juniper Networks Junos OS releases prior to 19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO.

CVE-2020-1648 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

There are no viable 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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
2020-07 Security Bulletin: Junos OS and Junos OS Evolved: RPD crash when processing a specific BGP packet (CVE-2020-1648) - Juniper Networks	Vendor Advisory kb.juniper.net text/html	CONFIRM kb.juniper.net/JSA11035

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	18.2x75	All	All	All
Operating System	Juniper	Junos	18.2x75	-	All	All
Operating System	Juniper	Junos	18.2x75	d20	All	All
Operating System	Juniper	Junos	18.2x75	d30	All	All
Operating System	Juniper	Junos	18.2x75	d40	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	20.1	r1	All	All
Operating System	Juniper	Junos	20.1	r1-s1	All	All
Operating System	Juniper	Junos	18.2x75	All	All	All
Operating System	Juniper	Junos	18.2x75	-	All	All
Operating	Juniper	Junos	18.2x75	d20	All	All

System						
Operating System	Juniper	Junos	18.2x75	d30	All	All
Operating System	Juniper	Junos	18.2x75	d40	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	20.1	r1	All	All
Operating System	Juniper	Junos	20.1	r1-s1	All	All
Operating System	Juniper	Junos Evolved	19.4	r1	All	All
Operating System	Juniper	Junos Evolved	19.4	r2	All	All
Operating System	Juniper	Junos Evolved	19.4	r2-s1	All	All
Operating System	Juniper	Junos Evolved	20.1	r1	All	All
Operating System	Juniper	Junos Evolved	19.4	r1	All	All
Operating System	Juniper	Junos Evolved	19.4	r2	All	All
Operating System	Juniper	Junos Evolved	19.4	r2-s1	All	All
Operating System	Juniper	Junos Evolved	20.1	r1	All	All
Operating System	Juniper	Junos Os Evolved	19.4	r1	All	All
Operating System	Juniper	Junos Os Evolved	19.4	r2	All	All
Operating System	Juniper	Junos Os Evolved	19.4	r2-s1	All	All
Operating System	Juniper	Junos Os Evolved	20.1	r1	All	All

cpe:2.3:o:juniper:junos:18.2x75:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:d20:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:d30:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:d40:*:*:*:*:*:*:

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

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:20.1:r1:*:*:*:*:*:*:

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

cpe:2.3:o:juniper:junos:18.2x75:*:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:-:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:d20:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:d30:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos:18.2x75:d40:*:*:*:*:*:*:

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:20.1:r1:*:*:*:*:*:*:

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

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

cpe:2.3:o:juniper:junos_evolved:19.4:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_evolved:19.4:r2-s1:*:*:*:*:*:*:

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

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

cpe:2.3:o:juniper:junos_evolved:19.4:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_evolved:19.4:r2-s1:*:*:*:*:*:*:

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

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

cpe:2.3:o:juniper:junos_os_evolved:19.4:r2:*:*:*:*:*:*:

cpe:2.3:o:juniper:junos_os_evolved:19.4:r2-s1:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

@RedPacketSec	CVE-2020-1648 - redpacketsecurity.com/cve-2020-1648/ #cybersecurity	2021-10-23 14:50:21
@softek_jp	Juniper Networks Junos OS の BGP の処理にサービスを妨害される問題 (CVE-2020-1648) [40331] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2021-10-25 02:30:40

← Previous ID

Next ID→