2021-10 Security Bulletin: Junos OS and Junos OS Evolved: RPD core upon receipt of specific BGP update (CVE-2021-31353)

Article ID JSA11218 **Created** 2021-09-28 **Last Updated** 2021-10-13

Product Affected

This issue affects specific versions of Junos OS and Junos OS Evolved (see below).

Severity	Severity Assessment (CVSS) Score
High	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Problem

An Improper Handling of Exceptional Conditions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an attacker to inject a specific BGP update, causing the routing protocol daemon (RPD) to crash and restart, leading to a Denial of Service (DoS).

Continued receipt and processing of the BGP update will create a sustained Denial of Service (DoS) condition.

This issue affects very specific versions of Juniper Networks Junos OS:

- 19.3R3-S2;
- 19.4R3-S3;
- 20.2 versions 20.2R2-S3 and later, prior to 20.2R3-S2;
- 20.3 versions 20.3R2 and later, prior to 20.3R3;
- 20.4 versions 20.4R2 and later, prior to 20.4R3;
- 21.1 versions prior to 21.1R2.

Juniper Networks Junos OS 20.1 is not affected by this issue.

This issue also affects Juniper Networks Junos OS Evolved:

- All versions prior to 20.4R2-S3-EVO, 20.4R3-EVO;
- 21.1-EVO versions prior to 21.1R2-EVO;
- 21.2-EVO versions prior to 21.2R2-EVO.

This issue can occur when multipath is enabled:

```
routing-instance <vrf> routing-options multipath
```

and one of the following two TTL propagation options (but *not* both) are enabled:

```
protocols mpls no-propagate-ttl
routing-instance <vrf> no-vrf-propagate-ttl
```

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

This issue was seen during production usage.

This issue has been assigned CVE-2021-31353 .

Solution

The following software releases have been updated to resolve this specific issue:

Junos OS 18.4R2-S9, 19.1R3-S7, 19.3R3-S3, 19.4R1-S4, 19.4R3-S4, 20.1R3, 20.2R3-S2, 20.3R3, 20.4R3, 21.1R2, 21.2R1, 21.2R2, 21.3R1, and all subsequent releases.

Junos OS Evolved 20.4R2-S3-EVO, 20.4R3-EVO, 21.1R2-EVO, 21.2R2-EVO, 21.3R1-EVO, and all subsequent releases.

Note: Only those releases listed in the PROBLEM section above are affected. This fix has also been proactively committed into other releases that are not vulnerable to this issue.

This issue is being tracked as 1595165 .

Software releases or updates are available for download at https://support.juniper.net/support/downloads/

Workaround

This issue can be mitigated in two ways:

1. ensure that TTL propagation is either enabled or disabled in both places below:

```
protocols mpls no-propagate-ttl
routing-instance <vrf> no-vrf-propagate-ttl
```

2. Disable multipath:

```
routing-instance <vrf> routing-options multipath
```

Modification History

```
2021-10-13: Initial Publication.
```

Related Information

- KB16613: Overview of the Juniper Networks SIRT Quarterly Security Bulletin Publication Process
- KB16765: In which releases are vulnerabilities fixed?
- KB16446: Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories
- Report a Vulnerability - How to Contact the Juniper Networks Security Incident Response Team
- CVE-2021-31353: RPD core upon receipt of specific BGP update

> AFFECTED PRODUCT SERIES / FEATURES

People also viewed