2022-01 Security Bulletin: Junos OS: Certificate validation is skipped when fetching system scripts from a HTTPS URL (CVE-2022-22156)

Article ID JSA11264 **Created** 2021-12-28

Last Updated 2022-01-12

Product Affected

This issue affects Junos OS all versions prior to 18.4R2-S9, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 20.4, 21.1.

Severity	Severity Assessment (CVSS) Score
Medium	6.5 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N)

Problem

An Improper Certificate Validation weakness in the Juniper Networks Junos OS allows an attacker to perform Person-in-the-Middle (PitM) attacks when a system script is fetched from a remote source at a specified HTTPS URL, which may compromise the integrity and confidentiality of the device.
The following command can be executed by an administrator via the CLI to refresh a script from a remote location, which is affected from this vulnerability:

```
>request system scripts refresh-from (commit | event | extension-service | op | snmp) file filename url <https-url>
```

This issue affects:
Juniper Networks Junos OS

- All versions prior to 18.4R2-S9, 18.4R3-S9;
- 19.1 versions prior to 19.1R2-S3, 19.1R3-S7;
- 19.2 versions prior to 19.2R1-S7, 19.2R3-S3;
- 19.3 versions prior to 19.3R3-S4;
- 19.4 versions prior to 19.4R3-S7;
- 20.1 versions prior to 20.1R2-S2, 20.1R3;
- 20.2 versions prior to 20.2R3;
- 20.3 versions prior to 20.3R2-S1, 20.3R3;
- 20.4 versions prior to 20.4R2;
- 21.1 versions prior to 21.1R1-S1, 21.1R2.

The examples of the config stanza affected by this issue:

```
[event-options event-script file <file-name> source <https-url> refresh]
[system scripts (commit | event | extension-service | op | snmp) file filena
refresh-from <https-url> ]
```

Please note that issuing set refresh-from command does not add the refresh-from statement to the confi
but the command behaves like an operational mode command by executing an operation.
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-2022-22156 .

Solution

The following software releases have been updated to resolve this specific issue: 18.4R2-S9, 18.4R3-S9, 19.1R2-S3, 19.1R3-S7, 19.2R1-S7, 19.2R3-S3, 19.3R3-S4, 19.4R3-S7, 20.1R2-S2, 20.1R3, 20.2R3, 20.3R2-S1, 20.3R3, 20.4R2, 21.1R1-S1, 21.1R2, 21.2R1 and all subsequent releases.
This issue is being tracked as 1542229 .
Software releases or updates are available for download at https://support.juniper.net/support/downloads/

Workaround

There are no viable workarounds for this issue.

Modification History

```
2022-01-12: 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 Security Vulnerability - How to Contact the Juniper Networks Security Incident Response Team
- CVE-2022-22156: Certificate validation is skipped when fetching system scripts from a HTTPS URL

AFFECTED PRODUCT SERIES / FEATURES