2021-10 Security Bulletin: SRC Series: NETCONF over SSH allows negotiation of weak ciphers (CVE-2021-31352)

Article ID JSA11217 **Created** 2021-09-28 **Last Updated** 2021-10-13

Product Affected

This issue affects SRC Series.

Severity	Severity Assessment (CVSS) Score
Medium	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Problem

An Information Exposure vulnerability in Juniper Networks SRC Series devices configured for NETCONF over SSH permits the negotiation of weak ciphers, which could allow a remote attacker to obtain sensitive information. A remote attacker with read and write access to network data could exploit this vulnerability to display plaintext bits from a block of ciphertext and obtain sensitive information.
This issue affects all Juniper Networks SRC Series versions prior to 4.13.0-R6.
A sample configuration of NETCONF over SSH is shown below:

```
netconf {
  ssh {
    port 830;
  }
}
```

Juniper SIRT is not aware of any malicious exploitation of this vulnerability.
This issue was found during internal product security testing or research.
This issue has been assigned CVE-2021-31352.

Solution

A hotfix has been created to resolve this issue. Contact Juniper Networks Technical Support to request the hotfix.
Weak ciphers are now disabled by default. Only the following ciphers and key-exchange (KEX) algorithms are now enabled by default:

- Ciphers: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
- KEX Algorithms: curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1

Note: After upgrading to a fixed release, any manually configured weak ciphers or KEX algorithms for NETCONF will be retained. Administrators should reset their cipher configuration by typing:

```
root@src# delete system services netconf ssh
root@src# commit
Stopping NETCONF/SSH:
commit complete.
root@src# set system services netconf ssh
```

This issue is being tracked as 1568322.

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

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-2021-31352: NETCONF over SSH allows negotiation of weak ciphers

AFFECTED PRODUCT SERIES / FEATURES

People also viewed