Juniper Networks | Support Portal

Product Affected

This issue affects all versions of Apstra.

Severity
High

Severity Assessment (CVSS) Score
CVSS: v3.1: 8.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N) **CVSS: v4.0:** 7 (CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:N/R:U/RE:M)

Problem

A Key Exchange without Entity Authentication vulnerability in the SSH implementation of Juniper Networks Apstra allows a unauthenticated, MITM attacker to impersonate managed devices.

Due to insufficient SSH host key validation an attacker can perform a machine-in-the-middle attack on the SSH connections from Apstra to managed devices, enabling an attacker to impersonate a managed device and capture user credentials.

This issue affects all versions of Apstra before 6.1.1.

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

This issue was discovered during external security research.

Solution

The following software releases have been updated to resolve this specific issue: Apstra 6.1.1, and all subsequent releases.

This issue is being tracked as as AOS-56131.

Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

Workaround

There are no known workarounds for this issue.

Severity Assessment

Information for how Juniper Networks uses CVSS can be found at KB 16446 "Common Vulnerability Scoring System (CVSS) and Juniper's Security Advisories."

Modification History

```
2026-04-08: 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

Acknowledgements

Juniper SIRT would like to acknowledge and thank the German Federal Office for Information Security (BSI) for responsibly reporting this vulnerability.

AFFECTED PRODUCT SERIES / FEATURES