Juniper Networks | Support Portal

Product Affected

This issue affects CTP OS 9.2.

Severity
High

Severity Assessment (CVSS) Score
CVSS: v3.1: 7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
CVSS: v4.0: 9.1 (CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/AU:Y/RE:M)

Problem

A Weak Password Requirements vulnerability in the password management function of Juniper Networks CTP OS might allow an unauthenticated, network-based attacker to exploit weak passwords of local accounts and potentially take full control of the device.

The password management menu enables the administrator to set password complexity requirements, but these settings are not saved. The issue can be verified with the menu option "Show password requirements". Failure to enforce the intended requirements can lead to weak passwords being used, which significantly increases the likelihood that an attacker can guess these and subsequently attain unauthorized access.

This issue affects CTP OS versions 9.2R1 and 9.2R2.

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

This issue was seen during production usage.

Solution

The following software releases have been updated to resolve this specific issue: 9.3R1, and all subsequent releases.

This issue is being tracked as 1924398 which is visible on the Customer Support website.

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

Workaround

Use access lists or firewall filters to limit access to the CLI only from trusted hosts and administrators.

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

AFFECTED PRODUCT SERIES / FEATURES