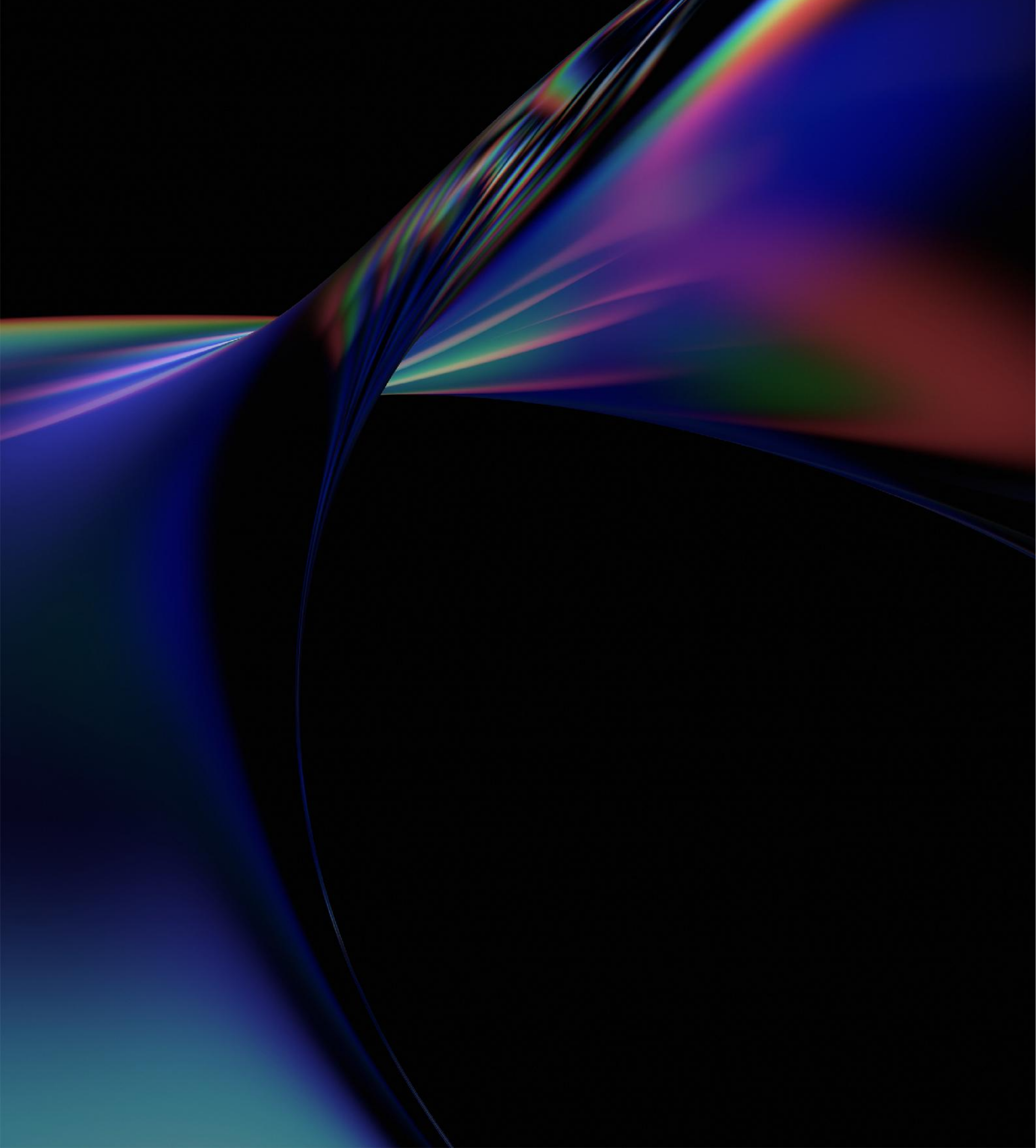
Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Vulnerability in Juniper Junos OS Evolved



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	31
Authors	Mihaela Matei <mihaela.matei@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-02-26
Issue Date	2026-02-26

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A critical vulnerability has been discovered in Junos OS Evolved network operating system running on PTX Series routers from Juniper Networks that could allow an unauthenticated attacker to execute code remotely with root privileges. Junos OS is an operating system that runs across all Juniper routing, switching, and security infrastructure.

PTX Series routers are high-performance core and peering routers built for high throughput, low latency, and scale. They are commonly used by internet service providers, telecommunication services, and cloud network applications.

RISK:

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

TECHNICAL SUMMARY:

CVE-2026-21902: (CVSS Score: 9.3)

An Incorrect Permission Assignment for Critical Resource vulnerability in the On-Box Anomaly detection framework of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated, network-based attacker to execute code as root. The On-Box Anomaly detection framework should only be reachable by other internal processes over the internal routing instance, but not over an externally exposed port. With the ability to access and manipulate the service to execute code as root a remote attacker can take complete control of the device.

Affected Versions and Solutions

Junos OS Evolved on PTX Series:

- 25.4 versions before 25.4R1-S1-EVO, 25.4R2-EVO.

Recommendations:

Smarttech247 team recommends the following actions to be taken:

1. **Apply** appropriate updates provided by Juniper to vulnerable systems immediately after appropriate testing. (M1051: Update Software)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process**: Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4**: **Perform Automated Application Patch Management**: Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets**: Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities**: Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date**: Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program**: Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scopes, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests**: Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise

and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.

   - Safeguard 18.3: Remediate Penetration Test Findings: Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

2. **Utilize** vulnerability scanning to find potentially exploitable software vulnerabilities to remediate them. (M1016: Vulnerability Scanning)
   - **Safeguard 16.13: Conduct Application Penetration Testing**: Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
3. **Apply** the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (M1026: Privileged Account Management)
   - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software**: Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include disabling default accounts or making them unusable.
   - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts**: Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

   - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts**: Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain the department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

4. **Safeguard 6.8: Define and Maintain Role-Based Access Control**: Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

References:

https://www.bleepingcomputer.com/news/security/critical-juniper-networks-ptx-flaw-allows-full-router-takeover/
https://supportportal.juniper.net/s/article/2026-02-Out-of-Cycle-Security-Bulletin-Junos-OS-Evolved-PTX-Series-A-vulnerability-allows-a-unauthenticated-network-based-attacker-to-execute-code-as-root-CVE-2026-21902
https://nvd.nist.gov/vuln/detail/CVE-2026-21902

CVE:

CVE-2026-21902

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com