Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Juniper Routers Auth Bypass Flaw Leads to Complete Device Takeover

Date of Publication	Admiralty Code	TA Number
July 3, 2024	A1	TA2024254

Summary

First Seen: June 2024
Affected Products: Session Smart Router, Session Smart Conductor, WAN Assurance Router
Impact: Juniper Networks has released an emergency patch to fix a critical vulnerability CVE-2024-2973 that allows authentication bypass in their products, including Session Smart Router (SSR), Session Smart Conductor, and WAN Assurance Router. This security flaw, could enable an attacker to gain complete control of the affected device.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-2973	Juniper Authentication Bypass Vulnerability	Session Smart Router, Session Smart Conductor, WAN Assurance Router	✗	✗	✓

Vulnerability Details

#1 Juniper Networks has issued critical security updates to address a serious vulnerability in some of its routers. tracked as CVE-2024-2973, this vulnerability has been assigned a CVSS score of 10.0, indicating its critical severity.

#2 The vulnerability arises from a lack of authentication checks when the router operates with a redundant peer. This oversight means that a remote attacker, without any authentication, could exploit the flaw to bypass security measures and gain complete control over the affected device. This could potentially compromise the device's security and integrity. Only routers or conductors running in high-availability redundant configurations are affected by this vulnerability.

#3 Juniper Networks has emphasized that applying the security fix should not disrupt normal network operations significantly. Users may experience approximately 30 seconds of downtime for web-based management and APIs during the update process. However, this short interruption is necessary to safeguard against the exploitation of the vulnerability.

#4 System administrators are strongly advised to promptly apply these security updates to their Juniper routers to mitigate the risk of unauthorized access and ensure the security of their network infrastructure. Taking swift action will help prevent potential security breaches and maintain the integrity of network operations.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-2973	Session Smart Router: All versions before 5.6.15, from 6.0 before 6.1.9-lts, from 6.2 before 6.2.5-sts; Session Smart Conductor: All versions before 5.6.15, from 6.0 before 6.1.9-lts, from 6.2 before 6.2.5-sts; WAN Assurance Router: 6.0 versions before 6.1.9-lts, 6.2 versions before 6.2.5-sts	cpe:2.3:h:juniper_networks:session_smart_conductor:*:*:*:*:*:*:*:* cpe:2.3:h:juniper_networks:session_smart_router:*:*:*:*:*:*:*:* cpe:2.3:h:juniper_networks:wan_assurance_router:*:*:*:*:*:*:*:*	CWE-288

Recommendations

Update: To mitigate this risk, Juniper has released updates for Session Smart Router in versions 5.6.15, 6.1.9-lts, and 6.2.5-sts. WAN Assurance Routers are automatically patched when connected to Mist Cloud. However, administrators of High-Availability clusters need to manually upgrade to SSR6.1.9 or SSR-6.2.5. In a Conductor-managed deployment, upgrading Conductor node is sufficient for mitigation.

Monitor Command Executions: To mitigate the risk of device takeover, implement continuous monitoring of login activities and device commands. This includes tracking and analyzing login attempts, command execution logs, and other device activities to detect anomalies.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0002** Execution	**TA0004** Privilege Escalation	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1068** Exploitation for Privilege Escalation	**T1059** Command and Scripting Interpreter	**T1059.008** Network Device CLI

Patch Details

To address the vulnerability (CVE-2024-2973), Juniper has released patched versions for Session Smart Router: 5.6.15, 6.1.9-lts, and 6.2.5-sts. WAN Assurance Routers receive automatic patches when connected to Mist Cloud. Administrators of High-Availability clusters must manually upgrade to SSR-6.1.9 or SSR-6.2.5. In Conductor-managed deployments, upgrading the Conductor node suffices for mitigation.

Links: https://support.juniper.net/support/downloads/

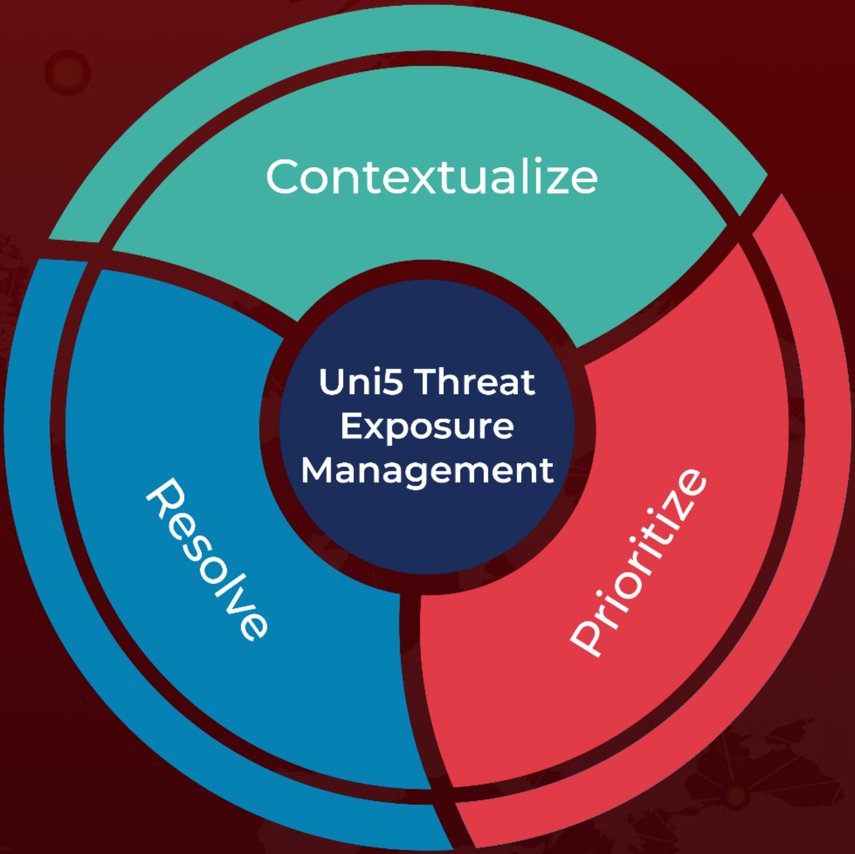
References

https://supportportal.juniper.net/s/article/2024-06-Out-Of-Cycle-Security-Bulletin-Session-Smart-Router-SSR-On-redundant-router-deployments-API-authentication-can-be-bypassed-CVE-2024-2973?language=en_US

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 3, 2024 • 7:00 AM

More at www.hivepro.com