# Advisory Alert

**Alert Number:** AAA20250110 **Date:** January 10, 2025

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Juniper** | **Critical** | Multiple Vulnerabilities |
| **Ubuntu** | **High** | Multiple Vulnerabilities |
| **Juniper** | **High , Medium** | Multiple Vulnerabilities |
| **Cisco** | **Medium** | Multiple Cross-Site Scripting Vulnerabilities |
| **VMware Broadcom** | **Medium** | Server Side Request Forgery Vulnerability |

## Description

| | |
|---|---|
| Affected Product | **Juniper** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-6119, CVE-2024-45492, CVE-2024-45491, CVE-2024-45490, CVE-2024-42131, CVE-2024-42102, CVE-2024-42096, CVE-2024-42082, CVE-2024-41096, CVE-2024-41073, CVE-2024-41055, CVE-2024-41044, CVE-2024-41040, CVE-2024-40936, CVE-2024-40927, CVE-2024-38619, CVE-2024-38559, CVE-2024-36979, CVE-2024-36883, CVE-2024-36019, CVE-2024-36000, CVE-2024-35875, CVE-2024-35797, CVE-2024-35791, CVE-2024-26946, CVE-2024-26886, CVE-2024-26720, CVE-2024-26630, CVE-2024-26629, CVE-2023-52801, CVE-2023-52463, CVE-2024-32462, CVE-2024-28834, CVE-2024-28835, CVE-2024-1488, CVE-2023-7008, CVE-2023-6240, CVE-2024-25742, CVE-2024-25743, CVE-2023-4408, CVE-2023-50387, CVE-2023-50868, CVE-2023-5517, CVE-2023-5679, CVE-2023-6516, CVE-2023-3019, CVE-2023-3255, CVE-2023-42467, CVE-2023-5088, CVE-2023-6683, CVE-2022-24810, CVE-2022-24809, CVE-2022-24808, CVE-2022-24807, CVE-2022-24806, CVE-2022-24805, CVE-2020-11022, CVE-2016-2183) |
| Description | Juniper has released security updates to address multiple vulnerabilities in their products. Exploitation of these vulnerabilities may lead to NULL pointer dereference, out-of-bounds access, cache corruption, use-after-free, denial of service.<br>Juniper advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Juniper Networks Junos Space versions prior to 24.1R2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R2-release?language=en_US |

| | |
|---|---|
| Affected Product | **Ubuntu** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to denial of service, sensitive information Disclosure, null pointer dereference, use after free<br>Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Ubuntu 22.04<br>Ubuntu 20.04 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://ubuntu.com/security/notices/USN-7186-2 |

| | |
|---|---|
| Affected Product | **Juniper** |
| Severity | **High** , **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-21602, CVE-2025-21593, CVE-2025-21592, CVE-2025-21600, CVE-2025-21596, CVE-2024-6387, CVE-2024-39894, CVE-2025-21599) |
| Description | Juniper has released security updates to address multiple vulnerabilities in their products. Exploitation of these vulnerabilities may lead to Denial of service, Exposure of Sensitive Information.<br><br>Juniper advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Junos OS<br>• All versions before:21.2R3-S9, 21.4R3-S9<br>• 22.2 before 22.2R3-S5<br>• 22.3 before 22.3R3-S4<br>• 22.4 before 22.4R3-S5<br>• 23.2 before 23.2R2-S3<br>• 23.4 before 23.4R2-S3<br>• 24.2 before 24.2R1-S2, 24.2R2<br>Junos OS Evolved<br>• All versions before:21.4R3-S9-EVO<br>• 22.2-EVO before 22.2R3-S5-EVO<br>• 22.3-EVO before 22.3R3-S4-EVO<br>• 22.4-EVO before 22.4R3-S5-EVO<br>• 23.2-EVO before 23.2R2-S2-EVO<br>• 23.4-EVO before 23.4R2-S2-EVO<br>• 24.2-EVO before 24.2R1-S2-EVO, 24.2R2-EVO<br><br>Junos OS SRX Series:<br>• All versions before 21.4R3-S8<br>• 22.2 before 22.2R3-S5<br>• 22.3 before 22.3R3-S3<br>• 22.4 before 22.4R3-S2<br>• 23.2 before 23.2R2-S1<br>• 23.4 before 23.4R2<br><br>Junos OS on SRX1500, SRX4100, SRX4200<br>• All versions before 21.4R3-S9<br>• 22.2 before 22.2R3-S5<br>• 22.3 before 22.3R3-S4<br>• 22.4 before 22.4R3-S4<br>• 23.2 before 23.2R2-S3<br>• 23.4 before 23.4R2-S1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Receipt-of-specially-crafted-BGP-update-packet-causes-RPD-crash-CVE-2025-21602?language=en_US<br>• https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-On-SRv6-enabled-devices-an-attacker-sending-a-malformed-BGP-update-can-cause-the-rpd-to-crash-CVE-2025-21593?language=en_US<br>• https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-SRX-Series-Low-privileged-user-able-to-access-highly-sensitive-information-on-file-system-CVE-2025-21592?language=en_US<br>• https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-With-certain-BGP-options-enabled-receipt-of-specifically-malformed-BGP-update-causes-RPD-crash-CVE-2025-21600?language=en_US<br>• https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-SRX1500-SRX4100-SRX4200-Execution-of-low-privileged-CLI-command-results-in-chassisd-crash-CVE-2025-21596?language=en_US<br>• https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-vulnerabilities-resolved-in-OpenSSH?language=en_US<br>• https://supportportal.juniper.net/s/article/2025-01-Security-Bulletin-Junos-OS-Evolved-Receipt-of-specifically-malformed-IPv6-packets-causes-kernel-memory-exhaustion-leading-to-Denial-of-Service-CVE-2025-21599?language=en_US |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Cross-Site Scripting Vulnerabilities (CVE-2025-20123, CVE-2025-20166, CVE-2025-20167 CVE-2025-20168) |
| Description | Cisco has released security updates to address multiple cross-site scripting (XSS) vulnerabilities in the web-based management interface of Cisco Common Services Platform Collector and Cisco Crosswork Network Controller. These vulnerabilities exist because the interface does not properly validate user-supplied input, allowing an authenticated, remote attacker to conduct XSS attacks.<br><br>Cisco advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Cisco Crosswork Network Controller Release before 5.0.4 , 6.0.3, 7.0.1<br>Cisco Common Services Platform Collector |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cspc-xss-CDOJZyH<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xwork-xss-KCcg7WwU#vp |

| | |
|---|---|
| Affected Product | **VMware Broadcom** |
| Severity | **Medium** |
| Affected Vulnerability | Server side request forgery vulnerability (CVE-2025-22215) |
| Description | Broadcom has released security updates addressing a server-side request forgery vulnerability in VMware Aria Automation and VMware Cloud Foundation. A malicious actor with 'Organization Member' access to Aria Automation may exploit this vulnerability to enumerate internal services running on the host/network.<br><br>Broadcom advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | VMware Aria Automation 8.x<br>VMware Cloud Foundation 5.x, 4.x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25312 |

**Disclaimer**

**The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.**