Advisory Alert

Alert Number: AAA20221013 **Date:** October 13, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
Juniper	**High**, **Medium**	Multiple Vulnerabilities
Redhat	**High**, **Medium**	Multiple Vulnerabilities
PaloAlto	**High**	Authentication Bypass Vulnerability

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2008-5161, CVE-2015-9262, CVE-2016-2124, CVE-2016-4658, CVE-2018-10689, CVE-2018-20532, CVE-2018-20533, CVE-2018-20534 ,CVE-2018-25032, CVE-2019-12735, CVE-2019-18282, CVE-2019-19532, CVE-2019-20811, CVE-2019-20934, CVE-2020-0427, CVE-2020-10769, CVE-2020-12362, CVE-2020-12363, CVE-2020-12364, CVE-2020-14314, CVE-2020-14351, CVE-2020-14385, CVE-2020-24394, CVE-2020-25211, CVE-2020-25212, CVE-2020-25643, CVE-2020-25645, CVE-2020-25656, CVE-2020-25705,CVE-2020-25709, CVE-2020-25710, CVE-2020-25717, CVE-2020-27170, CVE-2020-27777, CVE-2020-28374, CVE-2020-29661, CVE-2020-7053, CVE-2020-8648, CVE-2021-0543, CVE-2021-20265, CVE-2021-20271, CVE-2021-22543, CVE-2021-22555, CVE-2021-27363, CVE-2021-27364, CVE-2021-27365, CVE-2021-29154, CVE-2021-29650, CVE-2021-32399, CVE-2021-3347, CVE-2021-35550, CVE-2021-35556, CVE-2021-35559, CVE-2021-35561, CVE-2021-35564, CVE-2021-35565, CVE-2021-35567, CVE-2021-35578, CVE-2021-35586, CVE-2021-35588, CVE-2021-35603, CVE-2021-3653, CVE-2021-3656, CVE-2021-3715, CVE-2021-37576, CVE-2021-37750, CVE-2021-4034, CVE-2021-41617, CVE-2021-42574, CVE-2021-43527, CVE-2021-45417, CVE-2022-0778, CVE-2022-0847, CVE-2022-1271, CVE-2022-24407, CVE-2022-24903, CVE-2022-25235, CVE-2022-25236, CVE-2022-25315, CVE-2021-45960, CVE-2022-22823, CVE-2022-22824, CVE-2022-22822, CVE-2022-23852, CVE-2022-23990, CVE-2022-22825, CVE-2022-22826, CVE-2021-46143, CVE-2022-22827, CVE-2022-25314, CVE-2021-3711, CVE-2021-3712, CVE-2021-4160, CVE-2022-1292, CVE-2022-1343, CVE-2022-1434, CVE-2022-1473, CVE-2021-28165, CVE-2019-0205, CVE-2017-5929, CVE-2021-42550, CVE-2019-9518, CVE-2021-31535, CVE-2021-3177, CVE-2021-42771, CVE-2019-2435, CVE-2022-0492, CVE-2019-2684, CVE-2020-12321, CVE-2021-4155, CVE-2021-3573, CVE-2022-0330, CVE-2021-3752, CVE-2020-0465, CVE-2022-22942, CVE-2020-0466, CVE-2021-3564, CVE-2021-0920)
Description	Juniper has released security updates addressing multiple critical vulnerabilities that exist in their products. Successful exploitation of the most severe vulnerabilities can lead to integer overflow, buffer overflow, heap overflow, arbitrary code execution, denial of service and privilege escalation. Juniper highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Juniper Networks Session Smart Router All versions prior to 5.4.7 Juniper Networks Session Smart Router 5.5 versions prior to 5.5.3. Juniper Networks Steel Belted Radius Carrier Edition all versions prior to 8.6.0R16 on 64-bit Solaris Juniper Networks Steel Belted Radius Carrier Edition all versions prior to 8.6.0R16 on 64-bit Linux. Juniper Networks Contrail Networking version 2011 Junos Space all versions prior to 22.2R1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=date%20descending-&f:slevel=[Critical]

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-22225,CVE-2022-22247, CVE-2022-22218, CVE-2022-22201, CVE-2022-22224, CVE-2022-22223, CVE-2022-22249, CVE-2022-22211, CVE-2022-22192, CVE-2022-22251, CVE-2022-22220, CVE-2021-25220, CVE-2022-22199, CVE-2022-22239, CVE-2022-22237, CVE-2022-22232, CVE-2022-22226, CVE-2022-22228, CVE-2022-22235, CVE-2022-22234, CVE-2022-22248, CVE-2022-22250, CVE-2022-22240, CVE-2022-22229,CVE-2022-22231, CVE-2022-22230, CVE-2022-22208, CVE-2022-22241, CVE-2022-22242, CVE-2022-22243, CVE-2022-22244, CVE-2022-22245, CVE-2022-22246, CVE-2022-22238, CVE-2022-22236, CVE-2022-22227)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities can lead to denial of service, disclosure of private memory contents, system crash, privilege escalation, return of false information, unauthorized sessions, arbitrary command execution, memory corruption, cross-site scripting attacks, path injection and traversal, or local file inclusion Juniper highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#-sort=relevancy&f:slevel=[High,Medium]

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2588, CVE-2022-21123, CVE-2022-21125, CVE-2022-21166)
Description	Redhat has released a security update addressing multiple vulnerabilities that exist in the Red Hat Enterprise Linux. **CVE-2022-2588**- A use after free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local user to crash the system and possibly lead to a local privilege escalation problem. **CVE-2022-21123**- A flaw was found in hw. Incomplete cleanup of multi-core shared buffers for some Intel Processors may allow an authenticated user to enable information disclosure via local access. **CVE-2022-21125**- A flaw was found in hw. Incomplete cleanup of microarchitectural fill buffers on some Intel Processors may allow an authenticated user to enable information disclosure via local access. **CVE-2022-21166**- A flaw was found in hw. Incomplete cleanup in specific special register write operations for some Intel Processors may allow an authenticated user to enable information disclosure via local access. Redhat highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:6872

Affected Product	**PaloAlto**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2022-0030)
Description	Paloalto has released a security update addressing an Authentication Bypass vulnerability that exists in the Palo Alto Networks PAN-OS 8.1 web interface. A network-based attacker with specific knowledge of the target firewall or Panorama appliance can impersonate an existing PAN-OS administrator and perform privileged actions. Paloalto highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PAN-OS 8.1 versions prior to 8.1.24 including 8.1.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0030

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.