Advisory Alert

Alert Number: **AAA20240411** **Date:** **April 11, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	SQL Injection Vulnerability
Node.js	**High**	Command injection Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Palo Alto	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Juniper	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2011-1675, CVE-2011-1676, CVE-2011-1677, CVE-2016-2781, CVE-2017-18018, CVE-2018-1000215, CVE-2018-1000654, CVE-2018-20225, CVE-2018-20482, CVE-2018-7738, CVE-2019-17041, CVE-2019-17042, CVE-2019-18276, CVE-2019-9923, CVE-2020-14343, CVE-2020-19185, CVE-2020-19186, CVE-2020-19187, CVE-2020-19188, CVE-2020-19189, CVE-2020-19190, CVE-2020-22916, CVE-2020-25659, CVE-2020-27350, CVE-2020-27783, CVE-2020-28493, CVE-2020-28928, CVE-2020-36242, CVE-2020-8037, CVE-2021-20193, CVE-2021-22946, CVE-2021-22947, CVE-2021-23240, CVE-2021-28831, CVE-2021-28957, CVE-2021-30139, CVE-2021-33560, CVE-2021-34434, CVE-2021-36159, CVE-2021-37600, CVE-2021-40528, CVE-2021-41039, CVE-2022-3996, CVE-2022-4304, CVE-2022-4450, CVE-2022-48522, CVE-2022-48554, CVE-2023-0215, CVE-2023-0216, CVE-2023-0217, CVE-2023-0286, CVE-2023-0401, CVE-2023-0809, CVE-2023-1428, CVE-2023-2253, CVE-2023-23931, CVE-2023-2603, CVE-2023-2650, CVE-2023-27043, CVE-2023-28366, CVE-2023-29491, CVE-2023-32681, CVE-2023-32731, CVE-2023-32732, CVE-2023-3446, CVE-2023-3592, CVE-2023-36054, CVE-2023-38408, CVE-2023-3978, CVE-2023-39975, CVE-2023-40217, CVE-2023-41913, CVE-2023-43804, CVE-2023-44487, CVE-2023-46218, CVE-2023-4785, CVE-2023-4807, CVE-2023-48795, CVE-2023-49083, CVE-2023-5156, CVE-2023-5981, CVE-2024-30407, CVE-2023-38545, CVE-2023-38546, CVE-2023-23914, CVE-2023-23915, CVE-2020-8284, CVE-2020-8285, CVE-2020-8286, CVE-2018-1000120, CVE-2018-1000122)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Denial of service, Stack overflow, Memory leakage, NULL-pointer dereference Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of Junos OS before 23.4R1-S1, 23.4R2. All versions of Junos OS Evolved before 21.4R3-S4-EVO, 22.1-EVO, 22.3-EVO, 22.4-EVO. All versions of cRPD before 23.4R1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-cURL-vulnerabilities-resolved?language=en_US • https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-cRPD-Multiple-vulnerabilities-resolved-in-23-4R1-release?language=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2024-1597)
Description	IBM has released security updates addressing a SQL Injection Vulnerability that exists in the PostgreSQL JDBC Driver (PgJDBC). A remote attacker could send specially crafted SQL statements when using the non-default connection property preferQueryMode=simple in combination with application code that has a vulnerable SQL that negates a parameter value, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar Suite Software 1.10.12.0 - 1.10.19.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7147903

Affected Product	**Node.js**
Severity	**High**
Affected Vulnerability	Command Injection Vulnerability (CVE-2024-27980)
Description	Node.js has released security update for a Command injection Vulnerability, due to the improper handling of batch files in child_process.spawn / child_process.spawnSync. A malicious command line argument can inject arbitrary commands and achieve code execution even if the shell option is not enabled. Node.js recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Node.js release lines 18.x, 20.x, 21.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/april-2024-security-releases-2/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerability (CVE-2022-42896, CVE-2023-2002, CVE-2023-4623)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-42896** - A use-after-free flaw was found in the Linux kernel's implementation of logical link control and adaptation protocol (L2CAP), part of the Bluetooth stack in the l2cap_connect and l2cap_le_connect_req functions. An attacker with physical access within the range of standard Bluetooth transmission could execute code leaking kernel memory via Bluetooth if within proximity of the victim. **CVE-2023-2002** - A vulnerability was found in the HCI sockets implementation due to a missing capability check in net/bluetooth/hci_sock.c in the Linux Kernel. This flaw allows an attacker to unauthorized execution of management commands, compromising the confidentiality, integrity, and availability of Bluetooth communication. **CVE-2023-4623** - A use-after-free flaw was found in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component that can be exploited to achieve local privilege escalation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:1747 • https://access.redhat.com/errata/RHSA-2024:1746

Affected Product	**Palo Alto**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3385, CVE-2024-3382, CVE-2024-3384, CVE-2024-3386, CVE-2024-3387, CVE-2024-3388)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Denial of Service, Sensitive Information Disclosure, User Impersonation Palo Alto recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 10.0 Versions before 10.0.13 PAN-OS 10.1 Versions before 10.1.11-h4 PAN-OS 10.1 Versions before 10.1.12 on Panorama PAN-OS 10.1 Versions before 10.1.9-h3 PAN-OS 10.1 Versions before 10.1.12 PAN-OS 10.2 Versions before 10.2.7-h3 PAN-OS 10.2 Versions before 10.2.7-h3 on Panorama PAN-OS 10.2 Versions before 10.2.8 on Panorama PAN-OS 10.2 Versions before 10.2.4-h2 PAN-OS 10.2 Versions before 10.2.8 PAN-OS 11.0 Versions before 11.0.4 on Panorama PAN-OS 11.0 Versions before 11.0.1-h2 PAN-OS 11.0 Versions before 11.0.4 PAN-OS 11.1 Versions before 11.1.2 PAN-OS 8.1 Versions before 8.1.26 PAN-OS 9.0 Versions before 9.0.17-h4 PAN-OS 9.0 Versions before 9.0.17-h2 PAN-OS 9.0 Versions before 9.0.17 PAN-OS 9.1 Versions before 9.1.17 PAN-OS 9.1 Versions before 9.1.15-h1 Prisma Access Versions before 10.2.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-3385 • https://security.paloaltonetworks.com/CVE-2024-3382 • https://security.paloaltonetworks.com/CVE-2024-3384 • https://security.paloaltonetworks.com/CVE-2024-3386 • https://security.paloaltonetworks.com/CVE-2024-3387 • https://security.paloaltonetworks.com/CVE-2024-3388

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51775, CVE-2022-41723, CVE-2022-27664, CVE-2022-41721, CVE-2021-33194, CVE-2021-31525, CVE-2024-22234, CVE-2024-1597, CVE-2024-25710, CVE-2024-26308, CVE-2023-49083, CVE-2023-50782, CVE-2023-0286, CVE-2024-26130, CVE-2024-22195)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Attackers could exploit these vulnerabilities to cause Cross-site scripting, Denial of Service, Sensitive Information disclosure, Security restriction bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar Suite Software 1.10.12.0 - 1.10.19.0 IBM WebSphere Application Server Liberty 21.0.0.3 - 24.0.0.3 IBM WebSphere Application Server 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7147903 • https://www.ibm.com/support/pages/node/7147943

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Denial of service, Confidential information disclosure, Stack-based buffer overflow, Out-of-bounds read. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
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=%40sfcec_community_publish_date_formula__c%20descending&f:ctype= [Security%20Advisories]

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.