Advisory Alert

Alert Number: **AAA20230417** **Date:** **April 17, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Juniper	**High, Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**	Multiple Vulnerabilities
Ubuntu	**Medium, Low**	Multiple Vulnerabilities
Redhat	**Low**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-45960, CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852, CVE-2022-23990, CVE-2022-25235, CVE-2022-25236, CVE-2022-25313, CVE-2022-25314, CVE-2022-25315, CVE-2022-42889)
Description	Juniper has released security updates addressing multiple vulnerabilities that exists in Junos OS and Juniper Secure Analytics. If exploited these vulnerabilities could lead to integer overflow and remote code execution. Juniper highly recommends to apply necessary security fixes at earliest to avoid issues.

Affected Products	Junos OS All versions prior to 19.1R3-S10;
	Junos OS 19.4 versions prior to 19.4R3-S10;
	Junos OS 20.2 versions prior to 20.2R3-S6;
	Junos OS 20.3 versions prior to 20.3R3-S6;
	Junos OS 20.4 versions prior to 20.4R3-S5;
	Junos OS 21.1 versions prior to 21.1R3-S4;
	Junos OS 21.2 versions prior to 21.2R3-S4;
	Junos OS 21.3 versions prior to 21.3R3-S3;
	Junos OS 21.4 versions prior to 21.4R3-S1;
	Junos OS 22.1 versions prior to 22.1R2-S2, 22.1R3;
	Junos OS 22.2 versions prior to 22.2R2-S1, 22.2R3.
	Juniper Secure Analytics. Platforms: JSA Series versions prior to 7.5.0UP4.

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-JSA-Series-Apache-Commons-Text-prior-to-1-10-0-allows-RCE-when-applied-to-untrusted-input-due-to-insecure-interpolation-defaults-CVE-2022-42889?language=en_US https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-expat-resolved?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-5753, CVE-2021-3923, CVE-2021-4203, CVE-2022-20567, CVE-2023-0590, CVE-2023-1076, CVE-2023-1095, CVE-2023-1281, CVE-2023-1390, CVE-2023-1513, CVE-2023-23454, CVE-2023-23455, CVE-2023-28328, CVE-2023-28464, CVE-2023-28772)
Description	SUSE has release security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to stack information leak, use-after-free read flaw, NULL pointer dereference, denial of service, and buffer overflow. SUSE recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	openSUSE Leap 15.4 SUSE CaaS Platform 4.0 SUSE Linux Enterprise High Availability Extension 15 SP1 SUSE Linux Enterprise High Performance Computing 15 SP1 SUSE Linux Enterprise High Performance Computing 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Live Patching 15-SP1 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server 15 SP1 Business Critical Linux 15-SP1 SUSE Linux Enterprise Server 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Server for SAP Applications 15 SP1 SUSE Manager Proxy 4.0 SUSE Manager Retail Branch Server 4.0 SUSE Manager Server 4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20231848-1/

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1697, CVE-2023-28961, CVE-2023-28981, CVE-2023-28982, CVE-2023-28980, CVE-2023-28979, CVE-2023-28976, CVE-2023-28975, CVE-2023-28984, CVE-2023-28974, CVE-2023-28960, CVE-2023-28973, CVE-2023-28959, CVE-2023-28964, CVE-2023-28965, CVE-2023-28966, CVE-2023-28970, CVE-2023-28978, CVE-2023-28968, CVE-2023-28972, CVE-2023-28983, CVE-2023-28971, CVE-2023-22394)
Description	Juniper has released security updates addressing multiple Vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to Denial of Services, Shell Injection, Link Resolution Before File Access, Sequential Memory Allocation, and Improper Authentication. Juniper recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Junos OS, 20.1, 20.2, 20.3, 20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2. Affected platforms: PTX1000 Series, QFX10000 Series. All versions of Junos OS Evolved. All versions of Junos OS prior to 19.2, 19.3, 19.4, 20.1, 20.2, 20.3, 20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2, 22.3 on SRX Series using the JDPI-Decoder Engine on all versions prior to 5.7.0-47 with an AppID Service Sigpack prior to version 1.550.2-31. Affected platforms: SRX Series with IDP engine using AppID Service Sigpacks. All versions of Junos OS. All versions of Junos OS. Affected platforms: ACX Series. All versions of Junos OS. Affected platforms: MX Series. All versions of Junos OS. Affected platforms: QFX10002. Junos OS, 20.2, 20.3, 20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2. Affected platforms: QFX Series. Junos OS 19.2, 19.3, 19.4, 20.2, 20.4, 21.1, 21.2, 21.3, 21.4, 22.1, 22.2, 22.3. Affected platforms: NFX Series.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/global-search/%40uri?language=en_US#sort=relevancy&numberOfResults=25&f:ctype=[-%5BSecurity%20Advisories]&f:slevel=[High,Medium]&f:level1=[Security%20Advisories]

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0004, CVE-2023-0005, CVE-2023-0006)
Description	Palo Alto has release security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Local File Deletion and Sensitive Information disclosure. **CVE-2023-0004-** The vulnerability exists due to improper handling of exceptional condition. A remote authenticated administrator can delete files from the local file system with elevated privileges. **CVE-2023-0005-** The vulnerability exists due to missing encryption of sensitive information. A local administrator can obtain plaintext values of secrets stored in the device configuration and encrypted API keys. **CVE-2023-0006-** A local file deletion vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a user to delete system files from the endpoint with elevated privileges through a race condition. Palo Alto recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	GlobalProtect App 5.2 Before version5.2.13 on Windows GlobalProtect App 6.0 Before version6.0.4 on Windows GlobalProtect App 6.1Before version6.1.1 on Windows PAN-OS 10.0 Before version10.0.12 PAN-OS 10.1 Before version10.1.8 PAN-OS 10.2 Before version10.2.3 PAN-OS 8.1 Before version8.1.24 PAN-OS 9.0 Before version9.0.17 PAN-OS 9.1 Before version9.1.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-0005 https://security.paloaltonetworks.com/CVE-2023-0006 https://security.paloaltonetworks.com/CVE-2023-0004

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36516, CVE-2021-26401, CVE-2021-28711, CVE-2021-28712, CVE-2021-28713, CVE-2021-3428, CVE-2021-3659, CVE-2021-3669, CVE-2021-3732, CVE-2021-3772, CVE-2021-4149, CVE-2021-4203, CVE-2021-45868, CVE-2022-0487, CVE-2022-0494, CVE-2022-0617, CVE-2022-1016, CVE-2022-1195, CVE-2022-1205, CVE-2022-1462, CVE-2022-1516, CVE-2022-1974, CVE-2022-1975, CVE-2022-20132, CVE-2022-20572, CVE-2022-2196, CVE-2022-2318, CVE-2022-2380, CVE-2022-2503, CVE-2022-2663, CVE-2022-2991, CVE-2022-3061, CVE-2022-3111, CVE-2022-3303, CVE-2022-3628, CVE-2022-36280, CVE-2022-3646, CVE-2022-36879, CVE-2022-3903, CVE-2022-39188, CVE-2022-41218, CVE-2022-41849, CVE-2022-41850, CVE-2022-4382, CVE-2022-4662, CVE-2022-47929, CVE-2023-0394, CVE-2023-1074, CVE-2023-1095, CVE-2023-1118, CVE-2023-23455, CVE-2023-23559, CVE-2023-26545, CVE-2023-26607)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service, Memory exhaustion, Arbitrary code execution and Sensitive information disclosure. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6014-1 https://ubuntu.com/security/notices/USN-6020-1 https://ubuntu.com/security/notices/USN-6013-1

Affected Product	**Redhat**
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42252, CVE-2022-45143)
Description	Redhat has release security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to request smuggling and JsonErrorReportValve injection. **CVE-2022-42252-** The vulnerability exists in Apache Tomcat. If the server is configured to ignore invalid HTTP headers, the server does not reject a request containing an invalid content-length header, making it vulnerable to a request smuggling attack. **CVE-2022-45143-** A JsonErrorReportValve injection Vulnerability in the Tomcat package which allows users to input an invalid JSON structure, causing unwanted behavior as it did not escape the type, message, or description values**.** Redhat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 7 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1663 https://access.redhat.com/errata/RHSA-2023:1664

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.