Advisory Alert

Alert Number: AAA20241010 **Date:** October 10, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
Palo Alto	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Palo alto	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Hitachi	**High**, Medium, Low	Multiple Vulnerabilities
Juniper	**High**, Medium, Low	Multiple Vulnerabilities
Broadcom VMware	Medium	Multiple Vulnerabilities
Dell	Medium	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2016-0742, CVE-2016-0746, CVE-2016-0747, CVE-2016-1247, CVE-2016-4450, CVE-2017-7529, CVE-2017-20005, CVE-2018-16845, CVE-2019-20372, CVE-2021-3618, CVE-2021-23017, CVE-2022-41741, CVE-2022-41742, CVE-2023-44487)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service, NULL Pointer Dereference, Integer Overflow, Memory Disclosure. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following Junos OS configured with at least one of: webapi, or grpc telemetry. • All versions before 21.4R3-S8 • 22.2 versions before 22.2R3-S5 • 22.3 versions before 22.3R3-S3 • 22.4 versions before 22.4R3-S4 • 23.2 versions before 23.2R2-S2 • 23.4 versions before 23.4R2-S1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-10-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-OSS-component-nginx-resolved?language=en_US

Affected Product	**Palo Alto**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-9463, CVE-2024-9464, CVE-2024-9465, CVE-2024-9466, CVE-2024-9467)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Arbitrary code Execution, Information Disclosure, Cross Site Scripting. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Palo Alto Expedition prior to 1.2.96
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/PAN-SA-2024-0010

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Out-of-bounds Read, NULL Pointer Dereference, Double Free, permissions bypass. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP5, 15-SP6 Development Tools Module 15-SP5, 15-SP6 Legacy Module 15-SP5, 15-SP6 OpenSUSE Leap 15.6 OpenSUSE Leap Micro 5.5 SUSE Linux Enterprise Desktop 15 SP5, Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP2, 15 SP5, 15 SP6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP2, 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP2, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.1 to 5.5 SUSE Linux Enterprise Micro for Rancher 5.2 to 5.4 SUSE Linux Enterprise Real Time 15 SP5, 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP2, 15 SP5, 15 SP6 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5, 15 SP5, 15 SP6 SUSE Manager Proxy 4.1 SUSE Manager Retail Branch Server 4.1 SUSE Manager Server 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243559-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243561-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243563-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243565-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243567-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20243569-1

Affected Product	**Palo Alto**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-9471, CVE-2024-9473, CVE-2024-9470, CVE-2024-9469, CVE-2024-9468)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Memory Corruption Vulnerability, Denial of Service, Use After Free, Integer Overflow. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Palo Alto Prisma Access Browser prior to 129.59.2896.5 Palo Alto PAN-OS 11.1 prior to 11.1.3 Palo Alto PAN-OS 11.0 prior to 11.0.6 Palo Alto PAN-OS 10.2 prior to 10.2.11 Palo Alto PAN-OS 10.1 prior to 10.1.11 Palo Alto GlobalProtect App 6.3 All on Windows Palo Alto GlobalProtect App 6.2 prior to 6.2.5 on Windows Palo Alto GlobalProtect App 6.1 All on Windows Palo Alto GlobalProtect App 6.0 All on Windows Palo Alto GlobalProtect App 5.1 All on Windows Palo Alto Cortex XSOAR 6.12 prior to 6.12.0 (Build 1271551) Palo Alto Cortex XDR Agent 8.4 prior to 8.4.1 on Windows Palo Alto Cortex XDR Agent 8.3 prior to 8.3.1 on Windows Palo Alto Cortex XDR Agent 7.9-CE prior to 7.9.102-CE on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-9471 • https://security.paloaltonetworks.com/CVE-2024-9473 • https://security.paloaltonetworks.com/CVE-2024-9470 • https://security.paloaltonetworks.com/CVE-2024-9469 • https://security.paloaltonetworks.com/CVE-2024-9468

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Facets Module Versions prior to 2.0.9 Monster_menus module for Drupal 7.x Monster_menus module version 9.3.x Block_permissions module for Drupal 8.x Gutenberg module versions 8.x-2.x Gutenberg module versions 3.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-045 • https://www.drupal.org/sa-contrib-2024-046 • https://www.drupal.org/sa-contrib-2024-047 • https://www.drupal.org/sa-contrib-2024-048

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-15209, CVE-2023-25433, CVE-2023-52356, CVE-2023-6228, CVE-2024-24789, CVE-2024-39338, CVE-2024-42367, CVE-2022-24999, CVE-2023-50314, CVE-2024-34155, CVE-2024-34156, CVE-2024-34158, CVE-2024-38428, CVE-2024-41818, CVE-2023-26136, CVE-2024-6221, CVE-2024-5569, CVE-2024-34750)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak for Security Versions - 1.10.0.0 - 1.10.11.0 QRadar Suite Software Versions - 1.10.12.0 - 1.10.25.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7172678

Affected Product	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21416, CVE-2024-30073, CVE-2024-38014, CVE-2024-38045, CVE-2024-38046, CVE-2024-38119, CVE-2024-38217, CVE-2024-38234, CVE-2024-38235, CVE-2024-38237, CVE-2024-38238, CVE-2024-38239, CVE-2024-38240, CVE-2024-38241, CVE-2024-38242, CVE-2024-38243, CVE-2024-38244, CVE-2024-38245, CVE-2024-38246, CVE-2024-38247, CVE-2024-38248, CVE-2024-38249, CVE-2024-38250, CVE-2024-38252, CVE-2024-38254, CVE-2024-38256, CVE-2024-38257, CVE-2024-43461, CVE-2024-43487, CVE-2024-43491)
Description	Hitachi has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H Hitachi Virtual Storage Platform G1000, G1500 Hitachi Virtual Storage Platform F1500 Hitachi Virtual Storage Platform VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2024/09.html#references

Affected Product	**Juniper**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. 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]&f:slevel=[High,Low,Medium]

Affected Product	**Broadcom VMware**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38818, CVE-2024-38817, CVE-2024-38815)
Description	Broadcom has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware NSX - Version 3.x VMware NSX-T - Version 4.x VMware Cloud Foundation (NSX) - Version 4.x VMware Cloud Foundation (NSX-T) - Version 5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25047

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-50782, CVE-2023-52425, CVE-2024-39586)
Description	Dell has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC AppSync - Versions 4.3.0.0 through 4.6.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000234216/dsa-2024-420-security-update-for-dell-emc-appsync-for-multiple-vulnerabilities

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.