Advisory Alert

Alert Number: AAA20240711 **Date:** July 11, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
Palo Alto	**Critical**	Missing Authentication Vulnerability
VMware Broadcom	**Critical**	Multiple Vulnerabilities
VMware Broadcom	**High**	SQL-injection vulnerability
Cisco	**High**	Secure Boot Bypass Vulnerability
Dell	**High**	Multiple Vulnerabilities
NETGEAR	**High**, Medium	Multiple Vulnerabilities
Palo Alto	**High**, Medium	Multiple Vulnerabilities
Juniper	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2006-20001, CVE-2011-1473, CVE-2011-5094, CVE-2014-10064, CVE-2014-7191, CVE-2015-9262, CVE-2016-1000232, CVE-2016-10540, CVE-2016-4658, CVE-2017-1000048, CVE-2017-15010, CVE-2018-20834, CVE-2018-3737, CVE-2018-7408, CVE-2019-10081, CVE-2019-10082, CVE-2019-10092, CVE-2019-10097, CVE-2019-10098, CVE-2019-11719, CVE-2019-11727, CVE-2019-11756, CVE-2019-16775, CVE-2019-16776, CVE-2019-16777, CVE-2019-17006, CVE-2019-17023, CVE-2019-17567, CVE-2019-20149, CVE-2019-9517, CVE-2020-11668, CVE-2020-11984, CVE-2020-11993, CVE-2020-12362, CVE-2020-12400, CVE-2020-12401, CVE-2020-12402, CVE-2020-12403, CVE-2020-13938, CVE-2020-13950, CVE-2020-14145, CVE-2020-1927, CVE-2020-1934, CVE-2020-28469, CVE-2020-28502, CVE-2020-35452, CVE-2020-36049, CVE-2020-6829, CVE-2020-7660, CVE-2020-7754, CVE-2020-7774, CVE-2020-8648, CVE-2020-9490, CVE-2021-22543, CVE-2021-2342, CVE-2021-23440, CVE-2021-2356, CVE-2021-2372, CVE-2021-2385, CVE-2021-2389, CVE-2021-2390, CVE-2021-26690, CVE-2021-26691, CVE-2021-27290, CVE-2021-29469, CVE-2021-30641, CVE-2021-31535, CVE-2021-31618, CVE-2021-3177, CVE-2021-32803, CVE-2021-32804, CVE-2021-33033, CVE-2021-33034, CVE-2021-33193, CVE-2021-3347, CVE-2021-33909, CVE-2021-34798, CVE-2021-35604, CVE-2021-35624, CVE-2021-36160, CVE-2021-37701, CVE-2021-37712, CVE-2021-37713, CVE-2021-3803, CVE-2021-39275, CVE-2021-40438, CVE-2021-41524, CVE-2021-41773, CVE-2021-42013, CVE-2021-43527, CVE-2021-44224, CVE-2021-44790, CVE-2021-44906, CVE-2022-21245, CVE-2022-21270, CVE-2022-21303, CVE-2022-21304, CVE-2022-21344, CVE-2022-21367, CVE-2022-21417, CVE-2022-21427, CVE-2022-21444, CVE-2022-21451, CVE-2022-21454, CVE-2022-21460, CVE-2022-21589, CVE-2022-21592, CVE-2022-21595, CVE-2022-21608, CVE-2022-21617, CVE-2022-22719, CVE-2022-22720, CVE-2022-22721, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-23852, CVE-2022-23943, CVE-2022-25147, CVE-2022-25235, CVE-2022-25236, CVE-2022-2526, CVE-2022-25315, CVE-2022-26377, CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-29167, CVE-2022-29404, CVE-2022-30522, CVE-2022-30556, CVE-2022-31813, CVE-2022-3517, CVE-2022-3564, CVE-2022-36760, CVE-2022-37434, CVE-2022-37436, CVE-2022-40674, CVE-2022-46663, CVE-2023-0767, CVE-2023-21830, CVE-2023-21840, CVE-2023-21843, CVE-2023-21912, CVE-2023-21963, CVE-2023-21980, CVE-2023-22025, CVE-2023-22067, CVE-2023-22081, CVE-2023-22652, CVE-2023-24329, CVE-2023-25690, CVE-2023-2700, CVE-2023-27522, CVE-2023-2828, CVE-2023-30630, CVE-2023-32067, CVE-2023-32360, CVE-2023-32435, CVE-2023-32439, CVE-2023-3341, CVE-2023-34058, CVE-2023-34059, CVE-2023-34969, CVE-2023-3611, CVE-2023-37450, CVE-2023-3776, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-42753, CVE-2023-4863, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20932, CVE-2024-20945, CVE-2024-20952)
Description	Juniper has released a security update addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to denial of service, arbitrary code execution, privilege escalation, heap overflow. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Junos Space versions prior to 24.1R1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R1-release?language=en_US

Affected Product	**Palo Alto**
Severity	**Critical**
Affected Vulnerability	Missing Authentication Vulnerability (CVE-2024-5910)
Description	Palo Alto Networks has released a security update addressing a Missing Authentication Vulnerability that exists in Palo Alto Networks Expedition. Missing authentication for a critical function in Palo Alto Networks Expedition can lead to an Expedition admin account takeover for attackers with network access to Expedition. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Palo Alto Networks Expedition 1.2 versions below 1.2.92
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-5910

Affected Product	**VMware Broadcom**
Severity	**Critical -** Initial release date **6th March 2024 (AAA20240306)**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in VMware ESXi, Workstation and Fusion. Exploitation of these vulnerabilities may result in Code execution, Out of bound writes and Information disclosure. Broadcom recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	ESXi 8.0, 7.0 Workstation 17.x Cloud Foundation (ESXi) 5.x/4.x Fusion 13.x Running on MacOS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/24266

Affected Product	**VMware Broadcom**
Severity	**High**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2024-22280)
Description	Broadcom has released security updates addressing an SQL injection vulnerability that exists in VMware Aria Automation. Due to an incorrect input validation, An authenticated malicious user could enter specially crafted SQL queries and perform unauthorized read/write operations in the database. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Aria Automation 8.x 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/security-advisories/0/24598

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Secure Boot Bypass Vulnerability (CVE-2024-20456)
Description	Cisco has released security updates addressing a Secure Boot Bypass Vulnerability that exists in their products running on Cisco IOS XR Release. **CVE-2024-20456** - A vulnerability in the boot process of Cisco IOS XR Software could allow an authenticated, local attacker with high privileges to bypass the Cisco Secure Boot functionality and load unverified software on an affected device. To exploit this successfully, the attacker must have root-system privileges on the affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco products running Cisco IOS XR Release 24.2.1: • 8000 Series Routers • NCS 1010 Series Routers • NCS 1014 Series Routers • NCS 540 Series Routers that are running the NCS540L images • NCS 5700 Fixed Port Series Routers, excluding NCS-57C3-MOD-S and NCS-57C3-MOD-SE-S
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr-secure-boot-quD5g8Ap

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29966, CVE-2024-29968, CVE-2024-29969, CVE-2024-29963, CVE-2024-29961, CVE-2024-2859, CVE-2024-29960, CVE-2024-29959, CVE-2024-29958, CVE-2024-29957, CVE-2024-29950, CVE-2023-39417, CVE-2023-22006, CVE-2023-22036, CVE-2023-22041, CVE-2023-22043, CVE-2023-22044, CVE-2023-22045, CVE-2023-22049, CVE-2023-39410, CVE-2023-20861, CVE-2023-20863, CVE-2023-34478, CVE-2024-29965, CVE-2024-29962, CVE-2024-29956, CVE-2024-29955, CVE-2024-29952, CVE-2024-29951, CVE-2024-29967, CVE-2024-29964, CVE-2024-4173, CVE-2024-4161, CVE-2024-4159, CVE-2024-2860)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in third party components which affect Dell Connectrix (Brocade).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	Connectrix DS-300 Connectrix DS-6505B Connectrix DS-6510B Connectrix DS-6520B Connectrix DS-6610 Connectrix DS-6610B Connectrix DS-6620B Connectrix DS-6620B-V2 Connectrix DS-6630B Connectrix DS-6630B-V2 Connectrix DS-7720B Connectrix DS-7730B Connectrix ED-DCX6-4B Connectrix ED-DCX6-8B Connectrix ED-DCX7-4B Connectrix ED-DCX7-8B Connectrix ED-DCX8510-4B Connectrix ED-DCX8510-8B Connectrix MP-7810B Connectrix MP-7840B Connectrix MP-7850B
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000226794/dsa-2024-217-security-update-for-dell-connectrix-brocade-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000226842/dsa-2024-232-security-update-for-dell-connectrix-brocade-sannav-postgresql-vulnerability

Affected Product	**NETGEAR**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	NETGEAR has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to authentication bypass, Post-Authentication Buffer Overflow, Stored Cross Site Scripting, Post-Authentication Command Injection. NETGEAR advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NETGEAR Routers /Cable Modem Routers/ WiFi Systems • CAX30 firmware versions before 2.2.2.2 • MK62 firmware versions before 1.7.134 • MK72 firmware versions before 1.0.3.32 • MK82 firmware versions before 1.1.7.14 • MR60 firmware versions before 1.7.134 • MR70 firmware versions before 1.0.3.32 • MR80 firmware versions before 1.1.7.14 • MS60 firmware versions before 1.7.134 • MS70 firmware versions before 1.0.3.32 • MS80 firmware versions before 1.1.7.14 • R6700v3 firmware versions before 1.0.4.128 • R7000 firmware versions before 1.0.11.216 • R8000 firmware versions before 1.0.4.84 • RAX41 firmware versions before 1.0.16.132 • RAX42 firmware versions before 1.0.16.132 • RAX43 firmware versions before 1.0.16.132 • RAX50 firmware versions before 1.0.16.13 • RAX50S firmware versions before 1.0.16.132 • RAXE450 firmware versions before 1.0.12.96 • RAXE500 firmware versions before 1.0.12.96 • XR1000 firmware versions before 1.0.0.72
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://kb.netgear.com/000066265/Security-Advisory-for-Authentication-Bypass-on-Some-Cable-Modem-Routers-PSV-2023-0138 • https://kb.netgear.com/000066264/Security-Advisory-for-Stored-Cross-Site-Scripting-on-Some-Routers-PSV-2023-0122 • https://kb.netgear.com/000066263/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-Routers-PSV-2023-0119 • https://kb.netgear.com/000066262/Security-Advisory-for-Security-Misconfiguration-on-Some-Routers-PSV-2023-0116 • https://kb.netgear.com/000066261/Security-Advisory-for-Authentication-Bypass-on-Some-Routers-PSV-2023-0113 • https://kb.netgear.com/000066260/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2023-0079 • https://kb.netgear.com/000066259/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-and-WiFi-Systems-PSV-2022-0202 • https://kb.netgear.com/000066258/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2022-0201 • https://kb.netgear.com/000066257/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2022-0171

Affected Product	**Palo Alto**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3596, CVE-2024-5913, CVE-2024-5912, CVE-2024-5911)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Privilege Escalation, Improper Input Validation, Security bypass, arbitrary file upload. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cortex XDR Agent 8.2 Versions below 8.2.2 Cortex XDR Agent 7.9-CE Versions below 7.9.102-CE PAN-OS 10.1 Versions below 10.1.14 PAN-OS 10.1 Versions below 10.1.14-h2 PAN-OS 10.1 Versions below 10.1.9 on Panorama PAN-OS 10.2 Versions below 10.2.10 PAN-OS 10.2 Versions below 10.2.4 on Panorama PAN-OS 11.0 Versions below 11.0.4-h4 PAN-OS 11.0 Versions below 11.0.5 PAN-OS 11.1 Versions below 11.1.4 PAN-OS 11.2 Versions below 11.2.1 PAN-OS 9.1 Versions below 9.1.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-3596 • https://security.paloaltonetworks.com/CVE-2024-5913 • https://security.paloaltonetworks.com/CVE-2024-5912 • https://security.paloaltonetworks.com/CVE-2024-5911

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. If exploited, these vulnerabilities could lead to denial of service, arbitrary code execution, privilege escalation, heap overflow, memory leak. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of Junos OS and Junos OS Evolved. BBE Cloudsetup Versions before 2.1.0 Session Smart Router • All versions before SSR-5.6.14, • From 6.1 before SSR-6.1.8-lts, • From 6.2 before SSR-6.2.5-r2.
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]

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.