Advisory Alert

Alert Number: AAA20240530 **Date:** May 30, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Check Point	**High**	Information Disclosure Vulnerability
Citrix	**High**	Privilege Escalation Vulnerability
Drupal	**High**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities
nginx	**Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerStore Family. 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	PowerStore 500T PowerStoreT OS Versions prior to 4.0.0.0-2284811 PowerStore 1000T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 1200T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 3000T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 3200T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 5000T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 5200T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 7000T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 9000T PowerStoreT OSVersions prior to 4.0.0.0-2284811 PowerStore 9200T PowerStoreT OSVersions prior to 4.0.0.0-2284811
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000225368/dsa-2024-225-dell-powerstore-family-security-update-for-multiple-vulnerabilities

Affected Product	**Check Point**
Severity	**High**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-24919)
Description	Check Point has released a security update addressing an Information Disclosure Vulnerability that exists in their products. **CVE-2024-24919** - Vulnerability in Security Gateways with IPsec VPN, Remote Access VPN or the Mobile Access blade enabled. The vulnerability potentially allows an attacker to access information on Gateways connected to the Internet, with Remote Access VPN or Mobile Access enabled. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Quantum Security Gateway and CloudGuard Network Security: R81.20, R81.10, R81, R80.40 Quantum Maestro and Quantum Scalable Chassis: R81.20, R81.10, R80.40, R80.30SP, R80.20SP Quantum Spark Gateways: R81.10.x, R80.20.x, R77.20.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk182337

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2024-5027)
Description	Citrix has released a security update addressing a Privilege Escalation Vulnerability that exists in Citrix Workspace app for Mac. If exploited, an attacker with local authenticated user access to the device where CWA for Mac is installed can elevate privileges to a root user. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Citrix Workspace app for Mac before 2402.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX675851/citrix-workspace-app-for-mac-security-bulletin-for-cve20245027

Affected Product	**Drupal**
Severity	**High**
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 cause Cross Site Request Forgery and Access bypass. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Migrate queue importer module for Drupal 10 versions below 2.1.1 Image Sizes module for Drupal 10 versions below 3.0.2 Drupal REST & JSON API Authentication versions below 2.0.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-024 • https://www.drupal.org/sa-contrib-2024-023 • https://www.drupal.org/sa-contrib-2024-022

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51385, CVE-2023-48795)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2023-51385** - In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. **CVE-2023-48795 -** Terrapin Attack Vulnerability in SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking Aruba Switch Models: Aruba CX 10000 Switch Series Aruba CX 9300 Switch Series Aruba CX 8400 Switch Series Aruba CX 8360 Switch Series Aruba CX 8325 Switch Series Aruba CX 8320 Switch Series Aruba CX 6400 Switch Series Aruba CX 6300 Switch Series Aruba CX 6200 Switch Series Aruba CX 6100 Switch Series Aruba CX 6000 Switch Series Aruba CX 4100i Switch Series Running on Software Branch Versions: AOS-CX 10.13.xxxx: 10.13.1005 and below. AOS-CX 10.12.xxxx: 10.12.1021 and below. AOS-CX 10.10.xxxx: 10.10.1100 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesb3p04641en_us&docLocale=en_US

Affected Product	**nginx**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-31079, CVE-2024-32760, CVE-2024-34161, CVE-2024-35200)
Description	nginx has released a security update addressing multiple vulnerabilities that exist in their products. Multiple Vulnerabilities in nginx HTTP/3 implementation when nginx compiled with the experimental ngx_http_v3_module if the "quic" option of the "listen" directive is used in a configuration file. If exploited attacker can perform worker process crashes, worker process memory disclosure on systems with MTU larger than 4096 bytes, or might have a potential other impact using specially crafted QUIC session. nginx advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	nginx 1.25.0-1.25.5, 1.26.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mailman.nginx.org/pipermail/nginx-announce/2024/GMY32CSHFH6VFTN76HJNX7WNEX4RLHF6.html

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-25220, CVE-2022-2795, CVE-2022-3094, CVE-2022-48554, CVE-2022-48624, CVE-2023-2975, CVE-2023-3446, CVE-2023-3817, CVE-2023-4408, CVE-2023-5517, CVE-2023-5678, CVE-2023-5679, CVE-2023-6129, CVE-2023-6237, CVE-2023-6516, CVE-2023-7008, CVE-2023-7104, CVE-2023-45857, CVE-2023-47038, CVE-2023-50387, CVE-2023-50868, CVE-2023-52425, CVE-2024-0727, CVE-2024-2961, CVE-2024-22365, CVE-2024-25062, CVE-2024-25742, CVE-2024-25743, CVE-2024-28834, CVE-2024-28835, CVE-2024-33599, CVE-2024-33600, CVE-2024-33601, CVE-2024-33602, CVE-2021-47013, CVE-2023-3006, CVE-2023-52578, CVE-2024-26642, CVE-2024-26643, CVE-2024-26673, CVE-2024-26735, CVE-2024-26804, CVE-2024-26828, CVE-2024-26993)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist their products. These vulnerabilities could be exploited by malicious users to cause use-after-free, NULL Pointer Dereference, Integer Underflow, Reference leak. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Container Native Virtualization 4.14 for RHEL 9 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:3473 • https://access.redhat.com/errata/RHSA-2024:3461 • https://access.redhat.com/errata/RHSA-2024:3462 • https://access.redhat.com/errata/RHSA-2024:3460

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.