Advisory Alert

Alert Number: AAA20241114 **Date:** November 14, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HP	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**High**, **Medium**	Multiple Vulnerabilities
Lenovo	**Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Palo Alto	**Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**, **Low**	Multiple Vulnerabilities
F5	**Low**	SQLite Vulnerability
cPanel	**Low**	Security Update

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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 PowerProtect Cyber Recovery Versions prior to 19.17.0.2 Dell CyberSense Versions 8.0 through 8.9 Dell PowerProtect DD Versions 7.7.1 through 8.0.0.0 Dell PowerProtect DD Versions prior to 7.13.1.10 Dell PowerProtect DD Versions prior to 7.10.1.40 Dell PowerProtect DD Versions prior to 7.7.5.50 Dell PowerProtect DD Versions 7.8.0.0 through 8.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000247709/dsa-2024-435-security-update-for-dell-powerprotect-cyber-recovery-multiple-third-party-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000247827/dsa-2024-457-security-update-for-dell-cybersense-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000245360/dsa-2024-424-security-update-for-dell-pdsa-2024-424-security-update-for-dell-powerprotect-dd-vulnerabilityowerprotect-dd-vulnerability

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22185, CVE-2024-24985)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE StoreEasy servers using certain IBM processors. These vulnerabilities could be locally exploited to allow escalation of privilege. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE StoreEasy 1470 Storage - Prior to v2.30_08-09-2024 HPE StoreEasy 1470 Performance - Prior to v2.30_08-09-2024 HPE StoreEasy 1570 Storage - Prior to v2.30_08-09-2024 HPE StoreEasy 1570 Performance - Prior to v2.30_08-09-2024 HPE StoreEasy 1670 Performance Storage - Prior to v2.30_08-09-2024 HPE StoreEasy 1870 Storage - Prior to v2.30_08-09-2024 HPE StoreEasy 1870 Performance Storage - Prior to v2.30_08-09-2024 HPE StoreEasy 1670 Storage - Prior to v2.30_08-09-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04740en_us&docLocale=en_US

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 by malicious users to compromise the affected system. Suse advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5, 15.6 openSUSE Leap Micro 5.5 Public Cloud Module 15-SP5, 15-SP6 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15 SP5, 15 SP6 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP5, 15-SP6 SUSE Real Time Module 15-SP5, 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243986-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243985-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243984-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243983-1/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000219725/dsa-2024-009-security-update-for-dell-client-platform-for-multiple-amd-bios-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000216151/dsa-2024-027-security-update-for-dell-client-platform-amd-bios-vulnerability • https://www.dell.com/support/kbdoc/en-us/000212980/dsa-2024-029-security-update-for-an-amd-bios-vulnerability • https://www.dell.com/support/kbdoc/en-us/000225473/dsa-2024-241-security-update-for-dell-client-platform-for-IBM-ethernet-controller-and-adapter-software-advisories • https://www.dell.com/support/kbdoc/en-us/000226215/dsa-2024-281-security-update-for-dell-client-platform-for-multiple-openssl-vulnerabilities

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 to cause Cross Site Scripting, Arbitrary PHP code execution and Cross Site Scripting, Arbitrary PHP code execution. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	POST File module versions prior to 1.0.2 for Drupal 10.3.x/11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2024-060 • https://www.drupal.org/sa-contrib-2024-059

Affected Product	**Lenovo**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-23198, CVE-2024-28049, CVE-2024-25563, CVE-2024-24984)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in third-party products which in turn affect Lenovo products. These vulnerabilities could be exploited to cause denial of service or information disclosure. Lenovo 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://support.lenovo.com/us/en/product_security/LEN-158934

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52749,CVE-2024-26656,CVE-2024-26772,CVE-2024-26837,CVE-2024-26870,CVE-2024-26906,CVE-2024-26984,CVE-2024-31076,CVE-2024-35950,CVE-2024-38564,CVE-2024-38596,CVE-2024-40901,CVE-2024-40924,CVE-2024-40956,CVE-2024-40988,CVE-2024-41023,CVE-2024-41060,CVE-2024-41066,CVE-2024-46858,CVE-2024-42283,CVE-2024-46824)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial Of Service, Memory corruption, Use-After-Free conditions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:9605 • https://access.redhat.com/errata/RHSA-2024:9546

Affected Product	**Palo Alto**
Severity	**Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-2550, CVE-2024-2551, CVE-2024-2552, CVE-2024-5918, CVE-2024-5919, CVE-2024-9472, CVE-2024-5917, CVE-2024-5920)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service (DoS), Arbitrary File Delete, XML External Entities (XXE) injection, Server-Side Request Forgery Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 10.2 Versions Prior to 10.2.10-h7 PAN-OS 10.2 Versions Prior to 10.2.11-h4 PAN-OS 10.2 Versions Prior to 10.2.12 PAN-OS 10.2 Versions Prior to 10.2.4-h5 PAN-OS 10.2 Versions Prior to 10.2.4-h6 PAN-OS 10.2 Versions Prior to 10.2.5 PAN-OS 10.2 Versions Prior to 10.2.7-h16 PAN-OS 10.2 Versions Prior to 10.2.8-h13 PAN-OS 10.2 Versions Prior to 10.2.9-14 PAN-OS 11.0 Versions Prior to 11.0.6 PAN-OS 11.1 Versions Prior to 11.1.2-h14 PAN-OS 11.1 Versions Prior to 11.1.3-h10 PAN-OS 11.1 Versions Prior to 11.1.5 PAN-OS 11.2 Versions Prior to 11.2.2-h3 PAN-OS 11.2 Versions Prior to 11.2.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2024-2550 • https://security.paloaltonetworks.com/CVE-2024-2551 • https://security.paloaltonetworks.com/CVE-2024-2552 • https://security.paloaltonetworks.com/CVE-2024-5918 • https://security.paloaltonetworks.com/CVE-2024-5919 • https://security.paloaltonetworks.com/CVE-2024-9472 • https://security.paloaltonetworks.com/CVE-2024-5917 • https://security.paloaltonetworks.com/CVE-2024-5920

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45663, CVE-2024-37071, CVE-2024-41762, CVE-2024-41761, CVE-2024-40679, CVE-2024-7264)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial Of Service, Information Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 versions 11.1.4 - 11.1.4.7 IBM Db2 versions 11.5.0 - 11.5.9 IBM Db2 versions 10.5.0 - 10.5.11 IBM MaaS360 Cloud Extender Agent 2.89.000 - 3.000.900.017 IBM MaaS360 Cloud Extender Base Module 2.89.000 - 3.000.900.017
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7175943 • https://www.ibm.com/support/pages/node/7175940 • https://www.ibm.com/support/pages/node/7175946 • https://www.ibm.com/support/pages/node/7175947 • https://www.ibm.com/support/pages/node/7175957 • https://www.ibm.com/support/pages/node/7175929

Affected Product	**F5**
Severity	**Low**
Affected Vulnerability	SQLite Vulnerability (CVE-2020-13631)
Description	F5 has issued mitigations addressing a SQLite Vulnerability that exist in their products. The vulnerability allow a local, authenticated attacker with root-level privileges to exploit the vulnerability to modify SQLite files. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) Versions 17.1.0 - 17.1.1 BIG-IP (all modules) Versions 16.1.0 - 16.1.5 BIG-IP (all modules) Versions 15.1.0 - 15.1.10 BIG-IQ Centralized Management Versions 8.2.0 - 8.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000148494

Affected Product	**cPanel**
Severity	**Low**
Affected Vulnerability	Security Update (CVE-2024-9681)
Description	CPanel has released security updates addressing multiple vulnerabilities that exist in their cPanel EasyApache 4. CPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	cPanel curl 7.74.0 to and including 8.10.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-2024-11-13-maintenance-and-security-release/

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.