Advisory Alert

Alert Number: AAA20241118 **Date:** November 18, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Security Update
Dell	**Critical**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Kernel Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities
PostgreSQL	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-45490)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-45490 -** Multiple NetApp products incorporate libexpat. libexpat versions prior to 2.6.3 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20241018-0004/

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a monthly security update 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 Power Protect Data Manager - Versions prior to 19.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000248226/dsa-2024-461-security-update-for-dell-powerprotect-data-manager-multiple-third-party-component-vulnerabilities

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-51765, CVE-2024-51764)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-51765 -** A security vulnerability has been identified in HPE Cray Data Virtualization Service (DVS). Depending on configuration, this vulnerability may lead to local/cluster unauthorized access. **CVE-2024-51764 -** A security vulnerability has been identified in HPE Data Management Framework (DMF) Suite (CXFS). Depending on configuration, this vulnerability may lead to local/cluster unauthorized access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cray System Management Software prior to COS-2.5.146, COS 23.11.1, CLE 7.0.UP04.PS19 SGI CXFS prior to patch11804, patch11805, patch11806, patch11807
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04748en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04747en_us&docLocale=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Kernel Vulnerabilities (CVE-2024-42089, CVE-2024-43858, CVE-2024-27436, CVE-2024-26812, CVE-2024-39494, CVE-2024-38621, CVE-2024-26810, CVE-2024-38627, CVE-2024-39487, CVE-2024-42223, CVE-2024-42229, CVE-2024-46673, CVE-2024-38630, CVE-2024-42284, CVE-2024-44940, CVE-2024-41097, CVE-2024-42271, CVE-2024-42280, CVE-2023-52528, CVE-2024-38602)
Description	Ubuntu has released security updates addressing Kernel Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7110-1

Affected Product	**IBM**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2024-45087, CVE-2024-8096, CVE-2024-51462, CVE-2024-9681, CVE-2024-45296)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Malicious users could exploit these vulnerabilities to cause Cross-site Scripting, Inject XML, Denial of Service, Bypass Security Restrictions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server - Versions 9.0, 8.5 IBM QRadar WinCollect Agent- Versions 10.0-10.1.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7175393 • https://www.ibm.com/support/pages/node/7176043

Affected Product	**NetApp**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. Malicious users could exploit these vulnerabilities to cause Denial of Service, Disclosure of Sensitive Information, Addition or Modification of Data. NetApp 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://security.netapp.com/advisory/

Affected Product	**PostgreSQL**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-10976, CVE-2024-10977, CVE-2024-10978, CVE-2024-10979)
Description	PostgreSQL has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. PostgreSQL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PostgreSQL Versions – 12 to 17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.postgresql.org/support/security/CVE-2024-10976/ • https://www.postgresql.org/support/security/CVE-2024-10977/ • https://www.postgresql.org/support/security/CVE-2024-10978/ • https://www.postgresql.org/support/security/CVE-2024-10979/

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42283, CVE-2024-46824, CVE-2024-46858)
Description	Red Hat 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. 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:9605

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.