Advisory Alert

Alert Number: AAA20241220 **Date:** December 20, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Ubuntu	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**Medium**	Remote Authentication Bypass Vulnerability

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to memory leakage, use-after-free conditions, integer overflow, memory corruption, memory leakage, race conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Confidential Computing Module 15-SP6 SUSE Linux Enterprise High Availability Extension 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2, 15 SP6 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux SUSE Linux Enterprise Server 15 SP2 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP2, 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-20244388-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244387-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-51127, CVE-2024-4109)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-51127** - A flaw was found in Undertow. An HTTP request header value from a previous stream may be incorrectly reused for a request associated with a subsequent stream on the same HTTP/2 connection. This issue can potentially lead to information leakage between requests. **CVE-2024-4109** - A flaw was found in the createTempFile method of hornetq. Affected version of hornetq allows attackers to arbitrarily overwrite files or access sensitive information. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 9 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:11529 • https://access.redhat.com/errata/RHSA-2024:11531 • https://access.redhat.com/errata/RHSA-2024:11559 • https://access.redhat.com/errata/RHSA-2024:11560 • https://access.redhat.com/errata/RHSA-2024:11570

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26960, CVE-2024-26800, CVE-2024-27398, CVE-2024-50264, CVE-2024-26921, CVE-2024-43882, CVE-2024-38630)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 LTS Ubuntu 22.04 LTS Ubuntu 20.04 LTS Ubuntu 18.04 ESM Ubuntu 16.04 ESM Ubuntu 14.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0108-1

Affected Product	**Dell**
Severity	**High**
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 PowerStore 500T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 1000T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 1200T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 3000T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 3200T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 5000T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 5200T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 7000T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 9000T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell PowerStore 9200T - PowerStoreT OS Versions prior to 3.6.1.4-2413340 Dell Unisphere for PowerMax - Host Installation Versions prior to 9.2.4.12 DellUnisphere for PowerMax - Virtual Appliance Versions prior to 9.2.4.12 Dell Unisphere 360 - Host Installation Versions prior to 9.2.4.24 Dell Solutions Enabler Virtual Appliance Versions prior to 9.2.4.8 Dell PowerMax EEM - Embedded Management Versions prior to 55978.714.714.10632 Dell PowerMaxOS - PowerMax OS Version prior to 5978.714.714.10632 Dell VxFlex Ready Node in Dell PowerEdge BIOS-14G R640, R740, R840 Versions prior to 2.22.2 Dell PowerFlex Custom Node Dell PowerEdge BIOS-15G R650 and R750 Versions prior to 1.15.2 Dell PowerFlex Custom Node in Dell PowerEdge BIOS-15G AMD R6525 Versions prior to 2.16.3 Dell PowerFlex Custom Node in Dell PowerEdge BIOS-16G R660 and R760 Versions prior to 2.3.5 Dell PowerFlex Custom Node in Dell PowerEdge BIOS-16G AMD R6625 Versions prior to 1.9.5 Dell PowerFlex Custom Node in Dell PowerEdge BIOS-16G AMD R7625 Versions prior to 1.9.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000261519/dsa-2024-497-dell-powerstore-t-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000261502/dsa-2024-468-security-update-for-dell-powermaxos-5978-714-714-dell-unisphere-360-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-solutions-enabler-virtual-appliance-and-dell-powermax-eem-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000261944/dsa-2024-485-security-update-for-dell-vxflex-ready-node-and-powerflex-custom-node-multiple-third-party-component-vulnerabilities

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Remote Authentication Bypass Vulnerability (CVE-2023-52160)
Description	HPE has released security updates addressing a Remote Authentication Bypass vulnerability that exists in their products. **CVE-2023-52160** - The implementation of PEAP in wpa_supplicant through 2.10 allows authentication bypass. For a successful attack, wpa_supplicant must be configured to not verify the network's TLS certificate during Phase 1 authentication, and an eap_peap_decrypt vulnerability can then be abused to skip Phase 2 authentication. The attack vector is sending an EAP-TLV Success packet instead of starting Phase 2. This allows an adversary to impersonate Enterprise Wi-Fi networks. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE SANnav Management Software - Prior to v2.3.0a
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04766en_us&docLocale=en_US

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.