Advisory Alert

Alert Number: AAA20250211 **Date:** February 11, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Ubuntu	**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 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 Avamar Server Hardware Appliance Gen4T/ Gen5A Dell Avamar Virtual Edition Dell Avamar NDMP Accelerator Dell Avamar VMware Image Proxy Dell Networker Virtual Edition (NVE) Dell Power Protect DP Series Appliance / Dell Integrated Data Protection Appliance (IDPA)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000283460/dsa-2025-081-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-security-update-for-multiple-vulnerabilities

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 EMC Avamar Server Hardware Appliance Gen4S or Gen4T Dell EMC Avamar Virtual Edition Dell EMC Avamar NDMP Accelerator Dell EMC Avamar VMware Image Proxy Dell EMC NetWorker Virtual Edition (NVE) PowerStoreX OS Live Optics Collector Dell Enterprise SONiC Distribution
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000195194/dsa-2022-005-dell-emc-avamar-dell-emc-networker-virtual-edition-nve-and-dell-emc-powerprotect-dp-series-appliance-dell-emc-integrated-data-protection-appliance-idpa-security-update-for-multiple-vulnerabilities-os-security-rollup-2021r3 • https://www.dell.com/support/kbdoc/en-us/000242275/dsa-2024-432-dell-powerstore-x-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000281921/dsa-2025-076-security-update-for-dell-live-optics-collector-vulnerability • https://www.dell.com/support/kbdoc/en-us/000283465/dsa-2025-083-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53104, CVE-2024-53113)
Description	Red Hat has released Kernel security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to NULL pointer dereference and out-of-bounds write. **CVE-2024-53104 -** A vulnerability was found in the Linux kernel's USB Video Class driver. A buffer for video frame data is allocated, which does not account for all of the frame formats contained in a video stream, leading to an out-of-bounds write when a stream includes frames with an undefined format. **CVE-2024-53113-** The vulnerability in the Linux kernel involved a NULL pointer dereference in the alloc_pages_bulk_noprof() function. This occurred when a task was migrated between cpusets, causing a race condition in the prepare_alloc_pages() function. Specifically, the task's ac->nodemask could be modified concurrently, leading to an invalid preferred_zoneref value. When traversing the NUMA nodes, the incorrect ac->preferred_zoneref would point to a NULL zone, causing a NULL pointer dereference in alloc_pages_bulk_noprof() Red Hat 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://access.redhat.com/errata/RHSA-2025:1270 • https://access.redhat.com/errata/RHSA-2025:1269 • https://access.redhat.com/errata/RHSA-2025:1268 • https://access.redhat.com/errata/RHSA-2025:1267 • https://access.redhat.com/errata/RHSA-2025:1266 • https://access.redhat.com/errata/RHSA-2025:1264 • https://access.redhat.com/errata/RHSA-2025:1262 • https://access.redhat.com/errata/RHSA-2025:1254 • https://access.redhat.com/errata/RHSA-2025:1253

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41012,CVE-2024-42252,CVE-2024-53141,CVE-2024-40982,CVE-2024-43914,CVE-2024-41020,CVE-2024-42311,CVE-2024-41066,CVE-2024-38597,CVE-2024-38553)
Description	Ubuntu has released kernel security updates addressing several 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 ESM Ubuntu 14.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7262-1

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.