Advisory Alert

Alert Number: AAA20250516 **Date:** May 16, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Cisco	Medium	Arbitrary File Creation Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities in their products. If exploited, These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	RecoverPoint for Virtual Machines - Versions 6.0 SP1, 6.0 SP1 P1, 6.0 SP1 P2 and 6.0. SP2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000320811/dsa-2025-202-security-update-for-dell-recoverpoint-for-virtual-machines-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53141, CVE-2025-21756, CVE-2024-47745)
Description	Red Hat has released a security update addressing multiple vulnerabilities in their products. **CVE-2024-53141 -** In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. **CVE-2025-21756 -** A flaw was found in the Linux kernel's VMware network driver, where an improperly timed socket unbinding could result in a use-after-free issue. This flaw allows an attacker who can create and destroy arbitrary connections on virtual connections to read or modify system memory, potentially leading to an escalation of privileges or the compromise of sensitive data. **CVE-2024-47745 -** A flaw was found in the remap_file_pages function in mm/mmap.c in the Linux kernel, where it does not properly restrict execute access. This vulnerability allows local users to bypass intended SELinux W^X policy restrictions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64, TUS 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:7675 • https://access.redhat.com/errata/RHSA-2025:7676 • https://access.redhat.com/errata/RHSA-2025:7682

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28746, CVE-2023-32282, CVE-2023-22655, CVE-2024-42154, CVE-2024-38303, CVE-2024-38304)
Description	Dell has released a security update addressing multiple vulnerabilities in their products. If exploited, These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Disk Library for mainframe DLm8500 - Versions prior to 5.5.0.6 Disk Library for mainframe DLm2500 - Versions prior to 5.5.0.6 PowerSwitch Z9664F-ON Firmware - Versions prior to 3.54.5.1-9 Dell EMC Networking VEP1425/1445/1485 BIOS - Versions prior to 2.6 Dell SD-WAN EDGE620/640/680 BIOS - Versions prior to 3.50.0.9-21 Dell SD-WAN EDGE610/610-LTE BIOS - Versions prior to 3.43.0.9-24 PowerSwitch Z9432F-ON Firmware - Versions prior to 3.51.5.1-21 PowerSwitch Z9264F-ON Firmware - Versions prior to 3.42.5.1-21 PowerSwitch S5448F-ON Firmware - Versions prior to 3.52.5.1-12 PowerSwitch E3200-ON Series Firmware - Versions prior to 3.57.5.1-5 PowerSwitch N2200-ON Series Firmware - Versions prior to 3.45.5.1-31 PowerSwitch N3200-ON Series Firmware - Versions prior to 3.45.5.1-31
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000321646/dsa-2025-197-security-update-for-dell-networking-products-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000321651/dsa-2025-207-security-update-for-dell-disk-library-for-mainframe-vulnerabilities

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Arbitrary File Creation Vulnerability (CVE-2025-20187)
Description	Cisco has released security updates addressing an Arbitrary File Creation Vulnerability that exists in their products. **CVE-2025-20187 -** A vulnerability in the application data endpoints of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, remote attacker to write arbitrary files to an affected system. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Catalyst SD-WAN Manager Release prior to 20.9.7, 20.15.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanarbfile-2zKhKZwJ

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.