Advisory Alert

Alert Number: **AAA20250603** **Date:** **June 3, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Veritas Arctera	**Critical**	Multiple Vulnerabilities
Dell	**High**	Improper Link Resolution Vulnerability
Red Hat	**High**	Use-After-Free Vulnerability
Cisco	**High**, **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 third party products which affect Dell 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	Unisphere for PowerMax versions prior to 9.0.2.17 Unisphere for PowerMax Virtual Appliance versions prior to 9.0.2.17 Unisphere for PowerMax versions prior to 9.1.0.14 Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.14 Solutions Enabler versions prior to 9.0.0.18 Solutions Enabler Virtual Appliance versions prior to 9.0.0.18 Solutions Enabler versions prior to 9.1.0.5 Solutions Enabler Virtual Appliance versions prior to 9.1.0.5 PowerMax OS Release 5978
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000153922/dsa-2020-062-dell-emc-unisphere-for-powermax-unisphere-for-powermax-virtual-appliance-solutions-enabler-solutions-enabler-virtual-appliance-and-powermax-embedded-management-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Veritas Arctera**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38475, CVE-2025-24813)
Description	Arctera/Veritas has released security updates addressing multiple vulnerabilities that exist in third party products which affect Arctera/Veritas Desktop Laptop Option (DLO). **CVE-2024-38475** - Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. **CVE-2025-24813** - Path Equivalence: 'file.Name' (Internal Dot) leading to Remote Code Execution and other impacts have been found in Apache Tomcat 10.1.34 and earlier. The attack requires write enabled for the default servlet (disabled by default) - support for partial PUT (enabled by default) and other knowledge. Arctera/Veritas advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Arctera/Veritas Desktop Laptop Option (DLO) version 9.9 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veritas.com/support/en_US/security/ARC25-007

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Improper Link Resolution Vulnerability (CVE-2025-36564)
Description	Dell has released security updates addressing an Improper Link Resolution Vulnerability that exists in Dell Encryption Admin Utilities. **CVE-2025-36564** - Dell Encryption Admin Utilities versions prior to 11.10.2 contain an Improper Link Resolution vulnerability. A local malicious user could potentially exploit this vulnerability, leading to privilege escalation. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Encryption Admin Utilities Versions prior to 11.10.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000325203/dsa-2025-224

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Use-After-Free Vulnerability (CVE-2023-53107)
Description	Red Hat has released security updates addressing a Use-After-Free Vulnerability that exists in Red Hat Enterprise Linux kernel. **CVE-2023-53107** - A use-after-free vulnerability has been identified within the veth_convert_skb_to_xdp_buff() function of the Linux kernel's veth driver. Successful exploitation of this vulnerability could result in memory corruption, denial of service, and overall system instability. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:8399

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20509, CVE-2024-20498, CVE-2024-20499, CVE-2024-20500, CVE-2024-20501, CVE-2024-20502, CVE-2024-20513)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco Meraki MX and Z Series Teleworker Gateway AnyConnect VPN. These vulnerabilities could be exploited by malicious users to cause Denial of Service and Session Takeover. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following Cisco Meraki products if they are running on 16.2, 17, 18.1 and 18.2 releases of Cisco Meraki MX firmware and have Cisco AnyConnect VPN enabled: • MX64 • MX64W • MX65 • MX65W • MX67 • MX67C • MX67W • MX68 • MX68CW • MX68W • MX75 • MX84 • MX85 • MX95 • MX100 • MX105 • MX250 • MX400 • MX450 • MX600 • vMX • Z3 • Z3C • Z4 • Z4C
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-by-QWUkqV7X

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.