Advisory Alert

Alert Number: **AAA20250627** **Date:** **June 27, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Memory Overflow Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
F5	**Medium**	Information Disclosure Vulnerability

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 that 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 Secure Connect Gateway - Appliance - Versions prior to 5.30.0.14 Dell SRM - Windows/Linux update - Versions prior to 5.1.1.0 Dell Storage Monitoring and Reporting - Windows/Linux update - Versions prior to 5.1.1.0 Unisphere for PowerMax 9.2.4.17 - Host Installation - Versions prior to 9.2.4.17 Unisphere for PowerMax 10.2.0.12 - Host Installation - Versions prior to 10.2.0.12 Unisphere for PowerMax Virtual Appliance 9.2.4.17 - Virtual Appliance - Versions prior to 9.2.4.17 Unisphere 360 9.2.4.37 - Host Installation - Versions prior to 9.2.4.37 Solutions Enabler 9.2.4.11 - Host Installation - Versions prior to 9.2.4.11 Solutions Enabler 10.2.0.5 - Host Installation - Versions prior to 10.2.0.5 Solutions Enabler Virtual Appliance 9.2.4.11 - Virtual Appliance - Versions prior to 9.2.4.11 Dell PowerMax EEM 5978 - Embedded Management - Versions prior to 5978.714.714.10730 Dell PowerMaxOS 5978 - PowerMax OS - Version prior to 5978.714.714.10730 Dell PowerMax EEM 10.2.0.2 - Embedded Management - Version prior to 10.2.0.1 Patch 10732 Dell PowerMax OS 10.2.0.2 - PowerMax OS - Version prior to 10.2.0.1 Patch 10732 Power Protect Cyber Recovery - Cyber Recovery App Level Components - Versions prior to 19.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000337528/dsa-2025-260-dell-secure-connect-gateway-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000337550/dsa-2025-248-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000337554/dsa-2025-235-dell-powermaxos-dell-powermax-eem-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-unisphere-360-dell-solutions-enabler-and-dell-solutions-enabler-virtual-appliance-security-update-for-multiple-vulnerabilit • https://www.dell.com/support/kbdoc/en-us/000337700/dsa-2025-267-security-update-for-dell-powerprotect-cyber-recovery-multiple-third-party-component-vulnerabilities

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Memory Overflow Vulnerability (CVE-2025-6543)
Description	Citrix has released a security update addressing a memory overflow vulnerability that exists in their products. **CVE-2025-6543** - A vulnerability has been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway). Refer below for further details. Citrix advises to apply security fixes at your earliest to protect systems from potential threats
Affected Products	NetScaler ADC and NetScaler Gateway 14.1 Prior to 14.1-47.46 NetScaler ADC and NetScaler Gateway 13.1 Prior to 13.1-59.19 NetScaler ADC 13.1-FIPS and NDcPP Prior to 13.1-37.236-FIPS and NDcPP
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities that could be exploited by malicious users to compromise the affected system. SUSE 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://www.suse.com/support/update/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35857, CVE-2022-24805, CVE-2022-24806, CVE-2022-24807, CVE-2022-24808, CVE-2022-24809, CVE-2022-24810, CVE-2024-1737, CVE-2024-1975, CVE-2024-4076, CVE-2024-2236, CVE-2025-24970, CVE-2024-6119, CVE-2023-29483, CVE-2025-27152, CVE-2025-27789, CVE-2025-36038, CVE-2023-1667, CVE-2023-2283)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause null pointer dereference, improper input validation, server-side request forgery (SSRF) and improper authentication. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Virtualize - Versions 8.7 IBM QRadar Hub - Versions 1.0.0 - 3.8.2 IBM WebSphere Application Server - Versions 8.5, 9.0 IBM WebSphere Service Registry and Repository - Versions 8.5 IBM QRadar Deployment Intelligence App - Versions 1.0.0 - 3.0.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7237155 • https://www.ibm.com/support/pages/node/7238155 • https://www.ibm.com/support/pages/node/7238156 • https://www.ibm.com/support/pages/node/7237158 • https://www.ibm.com/support/pages/node/7237967 • https://www.ibm.com/support/pages/node/7238168

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2022-21233)
Description	F5 has released a security update addressing an information disclosure vulnerability that exists in their products. **CVE-2022-21233** - Improper isolation of shared resources in some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access. F5 advises to apply security fixes at your earliest to protect systems from potential threats
Affected Products	F5OS-A Versions - 1.8.0, 1.5.1 - 1.5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000152189

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.