Advisory Alert

Alert Number: AAA20250326 **Date:** March 26, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Privilege Escalation Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Broadcom VMware	**High**	Authentication Bypass Vulnerability
Dell	**High**, Medium	Multiple Vulnerabilities
HPE	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45745, CVE-2023-47855, CVE-2023-31355, CVE-2024-21978, CVE-2024-21980, CVE-2023-31315, CVE-2023-49141, CVE-2021-26344, CVE-2021-26387, CVE-2021-46772, CVE-2021-46746, CVE-2023-20518, CVE-2023-20578, CVE-2023-20584, CVE-2023-20591, CVE-2023-31356, CVE-2024-21981, CVE-2024-21801, CVE-2024-22374, CVE-2024-25943, CVE-2023-48795, CVE-2024-38433, CVE-2024-6387, CVE-2023-29499, CVE-2024-22273, CVE-2024-22274, CVE-2024-22275, CVE-2024-37086, CVE-2024-37087, CVE-2024-37085, CVE-2024-38812, CVE-2024-38813, CVE-2024-47176, CVE-2024-47076, CVE-2023-50782, CVE-2023-52425, CVE-2016-2183, CVE-2023-20608, CVE-2024-21094, CVE-2020-11023)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect PowerFlex appliance IC. 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	PowerFlex appliance Versions prior to IC 46.376.00 PowerFlex appliance Versions prior to IC 46.381.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000259574/dsa-2024-484-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-26512)
Description	NetApp has released security updates addressing a vulnerability that exists in SnapCenter. This vulnerability may allow an authenticated SnapCenter Server user to become an admin user on a remote system where a SnapCenter plug-in has been installed. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SnapCenter versions 6.0.1P1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250324-0001/

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-23450, CVE-2022-36364, CVE-2020-13936, CVE-2022-4883, CVE-2021-24032)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM and Storage Defender Resiliency Service. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, bypass security restrictions and Information Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5.0 - 7.5.0 UP4 IBM QRadar SIEM versions 7.4.3 GA - 7.4.3 FP8 IBM Storage Defender - Resiliency Service versions 2.0.0 - 2.0.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/6967333 • https://www.ibm.com/support/pages/node/7228988

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21785, CVE-2024-24857, CVE-2024-26733, CVE-2024-26851, CVE-2024-26940, CVE-2024-35854, CVE-2024-36901, CVE-2024-36920, CVE-2024-36927, CVE-2024-42084, CVE-2024-42265, CVE-2025-21785)
Description	Red Hat 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. 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-2025:3216 • https://access.redhat.com/errata/RHSA-2025:3215 • https://access.redhat.com/errata/RHSA-2025:3214 • https://access.redhat.com/errata/RHSA-2025:3211 • https://access.redhat.com/errata/RHSA-2025:3209 • https://access.redhat.com/errata/RHSA-2025:3207 • https://access.redhat.com/errata/RHSA-2025:3128 • https://access.redhat.com/errata/RHSA-2025:3127

Affected Product	**Broadcom VMware**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2025-22230)
Description	Broadcom has released security updates addressing an Authentication Bypass Vulnerability that exists in VMware Tools for Windows. **CVE-2025-22230** - VMware Tools for Windows contains an authentication bypass vulnerability due to improper access control. A malicious actor with non-administrative privileges on a Windows guest VM may gain ability to perform certain high-privilege operations within that VM. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Tools versions 12.x.x, 11.x.x for Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25518

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-5319, CVE-2020-16156, CVE-2023-31484, CVE-2024-52533, CVE-2015-20107, CVE-2020-10735, CVE-2021-3426, CVE-2021-3733, CVE-2021-3737, CVE-2021-4189, CVE-2021-28861, CVE-2021-29921, CVE-2022-42919, CVE-2022-45061, CVE-2023-6597, CVE-2023-24329, CVE-2023-27043, CVE-2023-40217, CVE-2024-0397, CVE-2024-0450, CVE-2024-4032, CVE-2024-6232, CVE-2024-6923, CVE-2024-7592, CVE-2024-8088, CVE-2024-9287, CVE-2024-11168, CVE-2024-38796)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell EMC Unity Family, Dell Precision Rack BIOS and third party products which affect Dell Enterprise SONiC Distribution. 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 Unity Operating Environment (OE) versions prior to 5.0.2.0.5.009 Dell EMC Unity XT Operating Environment (OE) versions prior to 5.0.2.0.5.009 Dell EMC Unity VSA Operating Environment (OE) versions prior to 5.0.2.0.5.009 Dell EMC VNX2 Operating Environment (OE) for File versions prior to 8.1.21.256 Dell EMC PowerMax eNAS versions prior to 8.1.13.504 and 8.1.14.532 Dell EMC PowerStore T versions prior to 1.0.1.0.5.002 Dell Enterprise SONiC Distribution versions prior to 4.4.2 Precision 7920 Rack BIOS versions prior to 2.23.0 Precision 7920 XL Rack BIOS versions prior to 2.23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000299082/dsa-2025-142-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000297542/dsa-2025-140 • https://www.dell.com/support/kbdoc/en-us/000001887/dsa-2020-019-dell-emc-unity-family-dell-emc-unity-xt-family-dell-emc-vnx2-family-dell-emc-powermax-embedded-nas-enas-and-dell-emc-powerstore-t-denial-of-service-vulnerability

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1053, CVE-2024-10404, CVE-2024-2240, CVE-2024-10405, CVE-2024-4282, CVE-2024-4317, CVE-2024-0985, CVE-2023-5870, CVE-2022-38178, CVE-2024-43796, CVE-2024-43799, CVE-2024-43800, CVE-2024-21538)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Disclosure of Information, Arbitrary file upload, Unquoted Search Path. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE SANnav Management Software - Prior to v2.3.1b and v2.4.0 HPE Unified OSS Console (UOC) versions prior to 3.1.14 - UOCCORE HPE Unified OSS Console Software Series versions prior to 3.1.14 - UOCAM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04817en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04834en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM and Storage Defender Resiliency Service. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, bypass security restrictions, Information Disclosure, Denial Of Service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5.0 - 7.5.0 UP4 IBM QRadar SIEM versions 7.4.3 GA - 7.4.3 FP8 IBM Storage Defender - Resiliency Service versions 2.0.0 - 2.0.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/6967333 • https://www.ibm.com/support/pages/node/7228988

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.