TLP: WHITE

Advisory Alert

Alert Number: AAA20260331 **Date:** March 31, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Buffer Overflow Vulnerability
Dell	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-26691, CVE-2024-7006, CVE-2025-29087, CVE-2025-3277, CVE-2025-6965, CVE-2022-1271, CVE-2025-30348, CVE-2021-42574, CVE-2019-1549, CVE-2019-1551, CVE-2020-1971, CVE-2021-23840, CVE-2021-23841, CVE-2021-3449, CVE-2021-3711, CVE-2021-3712, CVE-2021-4160, CVE-2022-1292, CVE-2022-2068, CVE-2022-2097, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-2650, CVE-2023-3446, CVE-2023-3817, CVE-2023-4807, CVE-2025-8576, CVE-2025-8577, CVE-2025-8578, CVE-2025-8579, CVE-2025-8580, CVE-2025-8581, CVE-2025-8582, CVE-2025-8583, CVE-2025-8879, CVE-2025-8880, CVE-2025-8881, CVE-2025-8882, CVE-2025-10500, CVE-2025-10501, CVE-2025-10502, CVE-2025-10585, CVE-2025-9864, CVE-2025-9865, CVE-2025-9866, CVE-2025-9867, CVE-2025-10200, CVE-2025-10201, CVE-2025-11211, CVE-2025-11458, CVE-2025-11460, CVE-2025-11205, CVE-2025-11206, CVE-2025-11207, CVE-2025-11208, CVE-2025-11209, CVE-2025-11210, CVE-2025-11212, CVE-2025-11213, CVE-2025-11215, CVE-2025-11216, CVE-2025-11219, CVE-2025-13042, CVE-2025-12036, CVE-2025-12428, CVE-2025-12429, CVE-2025-12430, CVE-2025-12431, CVE-2025-12432, CVE-2025-12433, CVE-2025-12434, CVE-2025-12435, CVE-2025-12436, CVE-2025-12437, CVE-2025-12438, CVE-2025-12439, CVE-2025-12440, CVE-2025-12441, CVE-2025-12443, CVE-2025-12444, CVE-2025-12445, CVE-2025-12446, CVE-2025-12447, CVE-2025-13226, CVE-2025-13227, CVE-2025-13228, CVE-2025-13229, CVE-2025-13230, CVE-2025-12725, CVE-2025-12726, CVE-2025-12727, CVE-2025-12728, CVE-2025-12729, CVE-2025-14174, CVE-2025-14372, CVE-2026-0628, CVE-2026-1861, CVE-2026-1862, CVE-2026-0899, CVE-2026-0900, CVE-2026-0901, CVE-2026-0902, CVE-2026-0903, CVE-2026-0904, CVE-2026-0905, CVE-2026-0906, CVE-2026-0907, CVE-2026-0908, CVE-2026-1220, CVE-2026-2441, CVE-2026-27171)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. 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	Wyse 5070 Thin Client • Version VMware_Horizon_ClientSDK_2406.8.13.0.47 and prior • Version Zoom_Universal_6.2.10.25600.2 and prior • Version Citrix_Workspace_App_24.11.0.85.113 and prior • Version Chrome_Browser_131.0.6778.204.3 and prior • Version ThinOS_2502_9.6.1080 and prior Wyse 5470 All-in-One Thin Client • Version Omnissa_Horizon_ClientSDK_2506.8.16.0_9 and prior • Version Zoom_Universal_6.4.10.26150.2 and prior • Version Citrix_Workspace_App_25.05.0.44.144 and prior • Version Chrome_Browser_138.0.7204.157.1 and prior • Version prior to ThinOS_2602_9.7.1008 Wyse 5470 Mobile Thin Client • Version Omnissa_Horizon_ClientSDK_2506.8.16.0_9 and prior • Version Zoom_Universal_6.4.10.26150.2 and prior • Version Citrix_Workspace_App_25.05.0.44.144 and prior • Version Chrome_Browser_138.0.7204.157.1 and prior • Version ThinOS_2602_9.7.1008 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000440831/dsa-2026-146

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-1188)
Description	IBM has released a security update addressing a vulnerability that exists in their Storage Protect products. **CVE-2026-1188**: In the Eclipse OMR port library component since release 0.2.0, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this function was incorrectly sized, failing to account for the separator when determining when a write to the buffer was safe could lead to a buffer overflow. This issue is fixed in Eclipse OMR version 0.8.0. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect for Virtual Environments: Data Protection for Hyper-V versions 8.1.0.0 to 8.2.0 IBM Storage Protect for Space Management versions 8.1.0.0 to 8.2.0 IBM Storage Protect for Virtual Environments: Data Protection for VMware versions 8.1.0.0 to 8.2.0 IBM Storage Protect Client versions 8.1.0.0 to 8.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7268095

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28047, CVE-2024-39279, CVE-2024-28956)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their PowerSwitch products. **CVE-2024-28047**: Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access. **CVE-2024-39279**: Insufficient granularity of access control in UEFI firmware in some Intel(R) processors may allow an authenticated user to potentially enable denial of service via local access. **CVE-2024-28956**: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerSwitch Z9664F-ON Firmware versions prior to 3.54.5.1-11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000446126/dsa-2026-162-security-update-for-dell-networking-products-for-z9664-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-4603, CVE-2025-53066, CVE-2025-53057, CVE-2024-6119, CVE-2024-56339, CVE-2024-9143, CVE-2025-36097, CVE-2025-48976, CVE-2025-7962, CVE-2024-2398, CVE-2025-36000, CVE-2025-36047, CVE-2025-36124, CVE-2024-5535, CVE-2020-36732, CVE-2025-12635, CVE-2024-9681, CVE-2024-2379, CVE-2024-13176, CVE-2024-2004, CVE-2026-21945, CVE-2026-21932, CVE-2026-21933, CVE-2026-21925, CVE-2024-2511, CVE-2024-2466, CVE-2025-68161, CVE-2025-48734, CVE-2024-8096)
Description	IBM has released a security update addressing multiple vulnerabilities that exists in Storage Protect products. These vulnerabilities could be exploited by malicious users to conduct Cross-Site Scripting, Out-of-bounds Read, Denial of Service, and Buffer Overflow attacks. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Protect for Virtual Environments: Data Protection for Hyper-V versions 8.1.0.0 to 8.2.0 IBM Storage Protect for Space Management versions 8.1.0.0 to 8.2.0 IBM Storage Protect for Virtual Environments: Data Protection for VMware versions 8.1.0.0 to 8.2.0 IBM Storage Protect Client versions 8.1.0.0 to 8.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7268095

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37849, CVE-2025-38141, CVE-2025-38248, CVE-2025-40096, CVE-2025-68349, CVE-2025-71085)
Description	Red Hat has released a security update addressing a vulnerability that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:6193

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.