Advisory Alert

Alert Number: AAA20250130 **Date:** January 30, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Use-after-free Vulnerability
Drupal	**High**	Access bypass vulnerability
Dell	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
cPanel	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38813, CVE-2024-38812, CVE-2024-37086, CVE-2024-37085, CVE-2023-3341, CVE-2023-28321, CVE-2023-46218, CVE-2023-28322, CVE-2023-38546, CVE-2023-34969, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2019-6470, CVE-2021-25217, CVE-2022-2928, CVE-2022-2929, CVE-2024-0553, CVE-2023-5981, CVE-2023-36054, CVE-2023-22084, CVE-2021-39537, CVE-2023-29491, CVE-2020-11080, CVE-2023-44487, CVE-2022-48565, CVE-2022-48560, CVE-2022-48564, CVE-2022-48566, CVE-2023-40217, CVE-2023-3446, CVE-2023-3817, CVE-2019-19333, CVE-2019-19334, CVE-2019-20393, CVE-2019-20394, CVE-2019-20397, CVE-2019-20391, CVE-2019-20392, CVE-2019-20395, CVE-2019-20396, CVE-2019-20398, CVE-2019-11324, CVE-2023-43804, CVE-2018-25091, CVE-2019-11236, CVE-2020-26137, CVE-2023-45803, CVE-2023-7090, CVE-2023-28486, CVE-2023-28487, CVE-2024-1975, CVE-2024-1737)
Description	Dell has released a security update addressing multiple vulnerabilities in third-party products, which, in turn, affect PowerProtect Data Protection Software. If exploited, malicious users could compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerProtect Data Protection Software- Integrated Data Protection - Versions prior to 2.7.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000278605/dsa-2025-039-security-update-for-dell-powerprotect-dp-series-appliance-idpa-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2019-13224)
Description	IBM has released a security update addressing A use-after-free vulnerability in IBM QRadar Assistant. **CVE-2019-13224 -** A use-after-free in onig_new_deluxe() in regext.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Assistant 1.0.0 - 3.8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7174015

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Access bypass vulnerability
Description	Drupal has released security updates addressing an access bypass vulnerability in the Authenticator Login component. Due to improper protection of custom paths, the module allows one user to access another user's two-factor configuration. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	alogin module 1.0.x alogin module 2.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2025-009

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23374, CVE-2024-1975, CVE-2024-1737, CVE-2023-45288, CVE-2023-48161, CVE-2022-28506, CVE-2021-40633, CVE-2024-33601, CVE-2024-33602, CVE-2024-2961, CVE-2024-33600, CVE-2024-33599, CVE-2022-41853, CVE-2024-3651, CVE-2024-28180, CVE-2023-50387, CVE-2023-50868, CVE-2023-6516, CVE-2023-4408, CVE-2023-5517, CVE-2022-2309, CVE-2024-37371, CVE-2024-37370, CVE-2024-21131, CVE-2024-21140, CVE-2024-21144, CVE-2024-21147, CVE-2024-21138, CVE-2024-21145, CVE-2024-5535, CVE-2021-3572, CVE-2023-5752, CVE-2020-14343, CVE-2020-25659, CVE-2023-52323, CVE-2023-32681, CVE-2024-31146, CVE-2024-31145, CVE-2024-42422)
Description	Dell has released security updates to address multiple vulnerabilities in their products. If exploited, these vulnerabilities could allow 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 Enterprise SONiC Distribution Versions prior to 4.4.1 Dell Enterprise SONiC Distribution Versions prior to 4.2.3 PowerStoreX OS Versions prior to 3.2.1.5-2424458 running on PowerStore 1000X, 3000X, 5000X, 7000X, 9000X Dell NetWorker Client Versions 19.11 through 19.11.0.2 Dell NetWorker Client Versions prior to 19.10.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000278568/dsa-2025-057-security-update-for-dell-enterprise-sonic-distribution-vulnerability • https://www.dell.com/support/kbdoc/en-us/000278110/dsa-2025-050-dell-powerstore-x-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000255892/dsa-2024-478-security-update-for-dell-networker-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47535, CVE-2019-19012, CVE-2019-16163, CVE-2022-24736, CVE-2022-24735, CVE-2022-24834, CVE-2023-45145, CVE-2023-28856, CVE-2023-52620, CVE-2023-52878, CVE-2024-26585, CVE-2023-52464, CVE-2023-52565, CVE-2023-52445, CVE-2024-35888, CVE-2024-36007, CVE-2023-52703, CVE-2024-26583, CVE-2024-36004, CVE-2024-26584, CVE-2024-35890, CVE-2024-26804, CVE-2023-38409, CVE-2024-35789, CVE-2024-35845, CVE-2023-52615, CVE-2023-39194, CVE-2024-26801, CVE-2023-52560, CVE-2023-52877, CVE-2023-52835, CVE-2023-52813, CVE-2023-52675, CVE-2023-52669, CVE-2022-48669, CVE-2021-46905, CVE-2023-52434, CVE-2024-26615, CVE-2023-52781, CVE-2024-26675, CVE-2024-35855, CVE-2024-26603, CVE-2024-35853, CVE-2024-0340, CVE-2024-26643, CVE-2024-26859, CVE-2024-26609, CVE-2024-26735, CVE-2024-26974, CVE-2024-35854, CVE-2023-52448, CVE-2023-6915, CVE-2023-6240, CVE-2023-52667, CVE-2023-39189, CVE-2024-26826, CVE-2024-26656)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause denial of services, information disclosure, arbitrary code execution, IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty 21.0.0.2 - 25.0.0.1 IBM QRadar Assistant 1.0.0 - 3.8.0 IBM Storage Copy Data Management 2.2.0.0 - 2.2.24.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7181925 • https://www.ibm.com/support/pages/node/7174015 • https://www.ibm.com/support/pages/node/7165417 • https://www.ibm.com/support/pages/node/7165416

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23083, CVE-2025-23084, CVE-2025-23085)
Description	cPanel has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to memory leaks, path traversal, and permission bypass. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache4 with vulnerable NodeJs versions All versions of NodeJS 18 through 18.20.5 All versions of NodeJS 20 through 20.18.1 All versions of NodeJS 22 through 22.13.0
Officially Acknowledged by the Vendor	Yes
`Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-4-maintenance-and-security-release/

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.