Advisory Alert

Alert Number: AAA20250318 **Date:** March 18, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**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 VxRail Appliance. 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 VxRail Appliance versions prior to 8.0.322 Dell VxRail Appliance with RecoverPoint for Virtual Machines Versions prior to 8.0.214 Dell VxRail Appliance Versions 7.0.000 through 7.0.540
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000294363/dsa-2025-115-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42159,CVE-2024-46815,CVE-2024-46818,CVE-2024-50302,CVE-2024-56648,CVE-2021-47496,CVE-2022-48792,CVE-2022-48911)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their SUSE Linux Enterprise products. These vulnerabilities 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	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250886-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250889-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250885-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250888-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250892-1/

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Networking OS10 10.5.6.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000295014/dsa-2025-068-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29041,CVE-2024-6221,CVE-2024-49766,CVE-2024-49767,CVE-2024-1135,CVE-2024-39689,CVE-2024-43799,CVE-2024-37891,CVE-2024-35195,CVE-2024-4340,CVE-2024-34069,CVE-2024-5569,CVE-2024-22195,CVE-2024-47764,CVE-2023-46136,CVE-2024-43796,CVE-2024-52798,CVE-2024-6345,CVE-2024-45590,CVE-2024-1681,CVE-2024-34064, CVE-2024-49822)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in their Product. If exploited, these vulnerabilities could lead to server-side request forgery, arbitrary code execution, denial of service, bypass security restrictions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Qradar Advisor 1.0.0 - 2.6.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7186423 • https://www.ibm.com/support/pages/node/7186424

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.