Advisory Alert

Alert Number:	AAA20250822	Date:	August 22, 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**, **Medium**	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 Dell VxRail Appliance. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell VxRail Appliance Versions 8.0.000 through 8.0.361
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000358419/dsa-2025-317-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36978, CVE-2025-21702, CVE-2025-37752, CVE-2025-37797, CVE-2025-38079, CVE-2025-38083, CVE-2025-38494, CVE-2025-38495)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. 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/announcement/2025/suse-su-202502955-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502945-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502944-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502943-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502942-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502938-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502937-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502936-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502934-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502933-1/

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaPay Pvt Ltd, 'The Zenith', 161A, Dharmapala Mawatha, Colombo 07, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public   Report incidents to incident@fincsirt.lk   TLP: WHITE

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38742, CVE-2025-38743)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-38742**- Dell iDRAC Service Module (iSM), versions prior to 6.0.3.0, contains an Incorrect Permission Assignment for Critical Resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution. **CVE-2025-38743**– Dell iDRAC Service Module (iSM), versions prior to 6.0.3.0, contains a Buffer Access with Incorrect Length Value vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution and Elevation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC Service Module Versions prior to 6.0.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000359617/dsa-2025-311-security-update-for-dell-idrac-service-module-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities CVE-2025-33120, CVE-2025-36042)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. **CVE-2025-33120**- IBM QRadar SIEM could allow an authenticated user to escalate their privileges via a misconfigured cronjob due to execution with unnecessary privileges. **CVE-2025-38743**– IBM QRadar Dashboard is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7242869

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.