Advisory Alert

Alert Number: **AAA20250729** **Date:** **July 29, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Palo Alto Networks	**Medium**	Incorrect Privilege Assignment Vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3596, CVE-2020-7105, CVE-2024-38428, CVE-2025-1795, CVE-2024-2398, CVE-2024-8096, CVE-2024-50602, CVE-2025-32414, CVE-2025-32415, CVE-2025-21605, CVE-2023-4738, CVE-2023-5344, CVE-2024-22667, CVE-2024-43802, CVE-2024-47814, CVE-2025-46836, CVE-2025-3576, CVE-2025-0395, CVE-2025-4802, CVE-2025-5222, CVE-2025-26476)
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 versions prior to 10.5.5.15 Dell ECS versions prior to 3.8.1.5 Dell ObjectScale version 4.0.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000350707/dsa-2025-284-security-update-for-dell-networking-os10-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000339134/dsa-2025-154-security-update-for-dell-ecs-and-objectscale-use-of-hard-coded-ssh-cryptographic-key-vulnerability

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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 system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 openSUSE Leap 15.4, 15.6 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP4, 15 SP6 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP6 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP6 SUSE Linux Enterprise Server 15 SP4, 15 SP6 SUSE Linux Enterprise Server 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502538-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502537-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48976, CVE-2025-48988, CVE-2025-49125, CVE-2025-52434, CVE-2025-52520, CVE-2025-53506)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in JBoss Enterprise Web Server. 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	JBoss Enterprise Web Server Text-Only Advisories x86_64 JBoss Enterprise Web Server 5 for RHEL 9 x86_64 JBoss Enterprise Web Server 5 for RHEL 8 x86_64 JBoss Enterprise Web Server 5 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:11696 • https://access.redhat.com/errata/RHSA-2025:11695

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-50181, CVE-2025-50182, CVE-2025-5889, CVE-2025-47278, CVE-2024-47081, CVE-2025-33097)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM. These vulnerabilities could be exploited by malicious users to cause Cross-site Scripting, Information Disclosure, Security Restrictions Bypass, unauthorized file modification. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP12 IF02 IBM QRadar Investigation Assistant versions 1.0.0 - 1.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7240798 • https://www.ibm.com/support/pages/node/7239755

Affected Product	**Palo Alto Networks**
Severity	**Medium**
Affected Vulnerability	Incorrect Privilege Assignment Vulnerability (CVE-2025-2179)
Description	Palo Alto Networks has released security updates addressing an Incorrect Privilege Assignment Vulnerability that exists in GlobalProtect App on Linux devices. **CVE-2025-2179** - An incorrect privilege assignment vulnerability in the Palo Alto Networks GlobalProtect App on Linux devices enables a locally authenticated non administrative user to disable the app even if the GlobalProtect app configuration would not normally permit them to do so. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GlobalProtect App 6.2 versions prior to 6.2.9 on Linux GlobalProtect App 6.1 all versions on Linux GlobalProtect App 6.0 all versions on Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2025-2179

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.