Advisory Alert

Alert Number: **AAA20240626** **Date:** **June 26, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Dell	**Medium**	TOCTOU Race Condition Vulnerability
IBM	**Medium**	Cross-Site Scripting Vulnerability

Description

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 cause Denial of Service, Use-after-free conditions, Memory leakage, NULL pointer dereference. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.4, 15.5 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Availability Extension 15 SP5 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4 and 5.5 SUSE Linux Enterprise Micro for Rancher 5.3 and 5.4 SUSE Linux Enterprise Real Time 15 SP4 and 15 SP5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 and 15 SP5 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 and 15 SP5 SUSE Linux Enterprise Workstation Extension 15 SP5 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/2024/suse-su-20242189-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242190-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242191-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242202-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242207-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242208-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242209-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242216-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242217-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242221-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-2002, CVE-2021-47400, CVE-2024-27393, CVE-2024-27397, CVE-2024-27403, CVE-2024-35870, CVE-2024-35958, CVE-2024-35960, CVE-2024-36957, CVE-2022-1048, CVE-2024-26642, CVE-2024-26993)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Privilege Escalation, Command Execution, System Crashes, Use-after-free Conditions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6/9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:4098 • https://access.redhat.com/errata/RHSA-2024:4106 • https://access.redhat.com/errata/RHSA-2024:4107 • https://access.redhat.com/errata/RHSA-2024:4108

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	TOCTOU Race Condition Vulnerability (CVE-2024-0171)
Description	Dell has released security updates addressing a TOCTOU Race Condition Vulnerability that exists in their products. A local low privileged attacker could potentially exploit this vulnerability to gain access to otherwise unauthorized resources. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerEdge C6615 BIOS Versions prior to 1.3.3 BIOS Versions prior to 1.8.3 in • PowerEdge R6615 • PowerEdge R7615 • PowerEdge R6625 • PowerEdge R7625 • Dell XC Core XC7625
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226253/dsa-2024-039-security-update-for-dell-amd-based-poweredge-server-vulnerability

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Cross-Site Scripting Vulnerability (CVE-2024-35153)
Description	IBM has released security updates addressing a Cross-Site Scripting Vulnerability that exists in IBM WebSphere Application Server. This vulnerability allows a privileged 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 WebSphere Application Server 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7158662

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.