Advisory Alert

Alert Number: AAA20250630 **Date:** June 30, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
IBM	**High**	Path Traversal Vulnerability
Red Hat	**Medium**	Security Update

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities (CVE-2022-49545, CVE-2024-40937, CVE-2024-50124, CVE-2024-50125, CVE-2024-50127, CVE-2024-50257, CVE-2024-50279, CVE-2024-50301, CVE-2024-53074, CVE-2024-53208, CVE-2024-56582, CVE-2024-56601, CVE-2024-56605)
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause use-after-free, out-of-bounds access, slab-use-after-free read. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.3, 15.4, 15.5, 15.6 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502145-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502146-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502154-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502155-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502156-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502157-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502161-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502162-1/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2019-20916)
Description	IBM has released security updates addressing a Path Traversal Vulnerability that exists in their products. **CVE-2019-20916** - The pip package before 19.2 for Python allows Directory Traversal when a URL is given in an install command, because a Content-Disposition header can have ../ in a filename, as demonstrated by overwriting the /root/.ssh/authorized_keys file. This occurs in _download_http_url in _internal/download.py. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM DB2 Data Management Console on CPD Versions - 4.8.6 or lower
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7238297

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2023-52933)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities that 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	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:9880

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.