Advisory Alert

Alert Number: AAA20250806 **Date:** August 6, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities
F5	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49058, CVE-2022-49788, CVE-2024-57980, CVE-2024-58002, CVE-2025-21727, CVE-2025-21905, CVE-2025-21928, CVE-2025-22004, CVE-2025-23150, CVE-2025-37738, CVE-2025-38052, CVE-2025-38089)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64, AUS 9.6 x86_64, TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:13061 • https://access.redhat.com/errata/RHSA-2025:13030 • https://access.redhat.com/errata/RHSA-2025:12977 • https://access.redhat.com/errata/RHSA-2025:12976

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21702, CVE-2025-37752, CVE-2025-37797, CVE-2024-53125, CVE-2024-56664, CVE-2024-26809, CVE-2024-41069)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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-202502710-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502708-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502707-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502704-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502699-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502698-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502697-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502693-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502689-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502691-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502688-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37797, CVE-2024-56748, CVE-2024-53239, CVE-2024-50073, CVE-2024-49950, CVE-2024-49883, CVE-2024-38541, CVE-2023-52975, CVE-2023-52885, CVE-2023-52757)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux Kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 16.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7685-1

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-26465, CVE-2024-13176, CVE-2025-40909, CVE-2025-29088, CVE-2025-3277, CVE-2025-29087, CVE-2024-56406, CVE-2024-55549, CVE-2025-24855, CVE-2024-56171, CVE-2025-24928, CVE-2025-27113)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial of service and potentially enable privilege escalation via local access. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale OneFS - Versions 9.5.0.0 through 9.10.1.2, Versions 9.11.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000353080/dsa-2025-272-security-update-for-dell-powerscale-onefs-multiple-third-party-component-vulnerabilities

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24806, CVE-2024-23306)
Description	F5 has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2024-24806** - This vulnerability could allow an attacker to launch Server-Side Request Forgery (SSRF) attacks by crafting payloads that resolve to unintended IP addresses, bypassing developer checks. **CVE-2024-23306** - An authenticated attacker may be able to modify or remove undisclosed configuration files causing a loss of confidentiality and integrity. This attack requires a privilege level that has access to stop and start services, so availability is not impacted. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) - 15.1.0 - 15.1.10, 16.1.0 - 16.1.6, 17.1.0 - 17.1.2, 17.5.0 - 17.5.1 BIG-IP Next CNF - 1.1.0 - 1.1.1 Traffix SDC - 5.1.0 F5OS-A - 1.4.0, 1.3.0 - 1.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000137886 • https://my.f5.com/manage/s/article/K000152876 • https://my.f5.com/manage/s/article/K000132686

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.