Advisory Alert

Alert Number: AAA20250715 **Date:** July 15, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Zyxel	**High**	Path Traversal Vulnerability

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49846, CVE-2024-10234, CVE-2025-2251, CVE-2025-2901, CVE-2025-23184, CVE-2025-35036, CVE-2025-48734)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Enterprise Linux and JBoss Enterprise Application Platform. 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 Application Platform Text-Only Advisories x86_64 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 8 ppc64le, 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64, 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 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 8.6 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 9.2 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 8 x86_64, 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64, 9.4 x86_64, 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le 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 9.2 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-2025:10931 • https://access.redhat.com/errata/RHSA-2025:10974 • https://access.redhat.com/errata/RHSA-2025:10976 • https://access.redhat.com/errata/RHSA-2025:10977 • https://access.redhat.com/errata/RHSA-2025:10978 • https://access.redhat.com/errata/RHSA-2025:10979 • https://access.redhat.com/errata/RHSA-2025:10980 • https://access.redhat.com/errata/RHSA-2025:10981

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-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP3, 15 SP7 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP7 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP3, SP7 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux SUSE Linux Enterprise Server 15 SP3 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP7 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502308-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502307-1/

Affected Product	**Zyxel**
Severity	**High**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2025-6265)
Description	Zyxel has released security updates addressing a Path Traversal Vulnerability that exists in Zyxel access point firmware. **CVE-2025-6265** - A path traversal vulnerability in the file_upload-cgi CGI program of certain AP firmware versions could allow an authenticated attacker with administrator privileges to access specific directories and delete files—such as the configuration file—on a vulnerable device. It is important to note that AP management interfaces are typically accessed within a LAN environment, and this attack would only be successful if strong, unique administrator passwords had already been compromised. Zyxel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NWA50AX firmware versions 7.10(ABYW.1) and earlier NWA50AX PRO firmware versions 7.10(ACGE.2) and earlier NWA55AXE firmware versions 7.10(ABZL.1) and earlier NWA90AX firmware versions 7.10(ACCV.1) and earlier NWA90AX PRO firmware versions 7.10(ACGF.2) and earlier NWA110AX firmware versions 7.10(ABTG.1) and earlier NWA130BE firmware versions 7.10(ACIL.2) and earlier NWA210AX firmware versions 7.10(ABTD.1) and earlier NWA220AX-6E firmware versions 7.10(ACCO.1) and earlier WAC500H firmware versions 6.70(ABWA.6) and earlier WAX300H firmware versions 7.10(ACHF.1) and earlier WAX510D firmware versions 7.10(ABTF.1) and earlier WAX610D firmware versions 7.10(ABTE.1) and earlier WAX620D-6E firmware versions 7.10(ACCN.1) and earlier WAX630S firmware versions 7.10(ABZD.1) and earlier WAX640S-6E firmware versions 7.10(ACCM.1) and earlier WAX650S firmware versions 7.10(ABRM.1) and earlier WAX655E firmware versions 7.10(ACDO.1) and earlier WBE530 firmware versions 7.10(ACLE.2) and earlier WBE660S firmware versions 7.10(ACGG.2) and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-path-traversal-vulnerability-in-aps-07-15-2025

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.