Advisory Alert

Alert Number: AAA20251003 **Date:** October 3, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
WordPress	**High**	Security Update
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**WordPress**
Severity	**High**
Affected Vulnerability	Security Update
Description	WordPress has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause data exposure and cross-site scripting. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress Versions - prior to 6.8.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2025/09/wordpress-6-8-3-release/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48913, CVE-2025-55163, CVE-2025-58056, CVE-2025-37823, CVE-2025-38200, CVE-2025-38449, CVE-2025-38472, CVE-2025-38500, CVE-2025-38527)
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 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 Server - AUS 9.4 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64, RHEL 9 x86_64 JBoss Enterprise Application Platform 8.1 for RHEL 8 x86_64, for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:17241 • https://access.redhat.com/errata/RHSA-2025:17298 • https://access.redhat.com/errata/RHSA-2025:17299 • https://access.redhat.com/errata/RHSA-2025:17317 • https://access.redhat.com/errata/RHSA-2025:17318

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38618, CVE-2025-38617, CVE-2025-38477, CVE-2025-37785, CVE-2025-21796, CVE-2024-49924, CVE-2024-35849, CVE-2024-27078, CVE-2021-47589, CVE-2021-47319, CVE-2021-47149)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7795-1 • https://ubuntu.com/security/notices/USN-7796-1 • https://ubuntu.com/security/notices/USN-7797-1

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.