Advisory Alert

Alert Number: AAA20260720 **Date:** July 20, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
WordPress	**Critical**	Remote Code Execution Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
WordPress	**Medium**	SQL Injection Vulnerability

Description

Vendor	**WordPress**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-63030)
Description	WordPress has released a security update addressing a vulnerability that exists in their products. **CVE-2026-63030:** WordPress versions 6.9 and higher are vulnerable to a REST API batch-route confusion weakness, which combined with an SQL injection issue leads to Remote Code Execution. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress versions: • 6.9.0 - 6.9.4 • 7.0.0 - 7.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31684, CVE-2026-43499, CVE-2026-46116, CVE-2026-53166, CVE-2026-46113, CVE-2026-53359)
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 systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 • Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 • Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.8 • Red Hat Enterprise Linux Server - TUS 8.8 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:41235 https://access.redhat.com/errata/RHSA-2026:41229

Vendor	**WordPress**
Severity	**Medium**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2026-60137)
Description	WordPress has released a security update addressing a vulnerability that exists in their products. **CVE-2026-60137:** WordPress 6.8.x before 6.8.6, 6.9.x before 6.9.5, and 7.0.x before 7.0.2 does not properly sanitise the author__not_in parameter of WP_Query, which could allow SQL Injection when a plugin or theme passes untrusted input to the parameter. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress versions: • 6.8.0 - 6.8.5 • 6.9.0 - 6.9.4 • 7.0.0 - 7.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2026/07/wordpress-7-0-2-release/

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.