Advisory Alert

Alert Number: AAA20260807 **Date:** August 7, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Sophos	**Critical**	Privilege Escalation Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
WordPress	**High**	Cross Site Scripting Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SonicWall	**Medium**	Scripting Syntax Vulnerability
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Virtual Storage Integrator for VMware vSphere Client - Versions prior to 10.11.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000496035/dsa-2026-335-security-update-for-dell-virtual-storage-integrator-for-vmware-vsphere-client-multiple-vulnerabilities

Vendor	**Sophos**
Severity	**Critical**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-18367)
Description	Sophos has released a security update addressing a vulnerability that exists in their products. **CVE-2026-18367:** A privilege escalation vulnerability allows local users to execute arbitrary code as root via Sophos Endpoint for macOS older than version 2026.1.1 and Sophos Home for macOS older than version 10.11.6. Sophos advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Sophos Intercept X Endpoint (Central) for macOS - Version 2026.1 and prior versions • Sophos Home for macOS - Version 10.11.5 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.sophos.com/en-us/security-advisories/sophos-sa-20260806-ep-macos-lpe

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-62718, CVE-2026-42264)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-62718:** Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.0 and 0.31.0, Axios does not correctly handle hostname normalization when checking NO_PROXY rules. Requests to loopback addresses like localhost. (with a trailing dot) or [::1] (IPv6 literal) skip NO_PROXY matching and go through the configured proxy. This goes against what developers expect and lets attackers force requests through a proxy, even if NO_PROXY is set up to protect loopback or internal services. This issue leads to the possibility of proxy bypass and SSRF vulnerabilities allowing attackers to reach sensitive loopback or internal services despite the configured protections. **CVE-2026-42264:** Axios is a promise based HTTP client for the browser and Node.js. From version 1.0.0 to before version 1.15.2, fFive config properties (auth, baseURL, socketPath, beforeRedirect, and insecureHTTPParser) in the HTTP adapter are read via direct property access without hasOwnProperty guards, making them exploitable as prototype pollution gadgets. When Object.prototype is polluted by another dependency in the same process, axios silently picks up these polluted values on every outbound HTTP request. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security Verify Information Queue Version: • 10.0.9 • 10.0.8 • 10.0.7 • 10.0.6 • 10.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7282720

Vendor	**WordPress**
Severity	**High**
Affected Vulnerability	Cross Site Scripting Vulnerability (CVE-2026-64638)
Description	WordPress has released a security update addressing a vulnerability that exists in their products. **CVE-2026-64638:** WordPress is vulnerable to a pre-auth reflected XSS vulnerability on the login screen. Via a specially crafted malicious third-party website hosted by an attacker, it is possible for this to be escalated to an RCE vulnerability with conditions outside of the attackers control. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress Affected Versions: • 7.0.0 - 7.0.2 • 6.9.0 - 6.9.5 • 6.8.0 - 6.8.6 • 6.7.0 - 6.7.5 • 6.6.0 - 6.6.5 • 6.5.0 - 6.5.8 • 6.4.0 - 6.4.8 • 6.3.0 - 6.3.8 • 6.2.0 - 6.2.9 • 6.1.0 - 6.1.10 • 6.0.0 - 6.0.12 • 5.9.0 - 5.9.13 • 5.8.0 - 5.8.13 • 5.7.0 - 5.7.15 • 5.6.0 - 5.6.17 • 5.5.0 - 5.5.18 • 5.4.0 - 5.4.19 • 5.3.0 - 5.3.21 • 5.2.0 - 5.2.24 • 5.1.0 - 5.1.22 • 5.0.0 - 5.0.25 • 4.9.0 - 4.9.29 • 4.8.0 - 4.8.28 • 4.7.0 - 4.7.33
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2026/08/wordpress-7-0-3-release/

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-25639, CVE-2026-67312, CVE-2026-67313, CVE-2026-67316, CVE-2026-67317, CVE-2026-67319, CVE-2025-58754, CVE-2026-40175, CVE-2025-15284, CVE-2026-8723, CVE-2026-2391, CVE-2026-33671, CVE-2026-33672, CVE-2026-4867, CVE-2026-39865, CVE-2025-69873, CVE-2024-6763, CVE-2026-44486, CVE-2026-44487, CVE-2026-44488, CVE-2026-44490, CVE-2026-44492, CVE-2026-44494, CVE-2026-44495, CVE-2026-44496, CVE-2026-11714, CVE-2026-15328, CVE-2026-14981, CVE-2026-15064, CVE-2026-15325, CVE-2026-59879, CVE-2026-59880, CVE-2026-34282, CVE-2026-22016, CVE-2026-23865, CVE-2026-22021, CVE-2026-22013, CVE-2026-22018, CVE-2026-34268, CVE-2026-22007)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere Application Server - Versions 8.5 & 9.0 WebSphere Application Server Liberty - Versions 17.0.0.3 - 26.0.0.7 Platform Navigator in IBM Cloud Pak for Integration (CP4I) - Version 16.2.0 to 16.2.0.1 IBM Knowledge Catalog Neo4j On Cloud Pak for Data - Versions 5.0.0 to 5.3.1 patch 3 IBM Security Verify Information Queue Version: • 10.0.9 • 10.0.8 • 10.0.7 • 10.0.6 • 10.0.5 IBM Master Data Management (formerly known as IBM Match 360) On Cloud Pak for Data - Versions 5.1.3 to 5.3.1 patch 3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7278580 • https://www.ibm.com/support/pages/node/7281625 • https://www.ibm.com/support/pages/node/7282767 • https://www.ibm.com/support/pages/node/7282721 • https://www.ibm.com/support/pages/node/7282720

Vendor	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Scripting Syntax Vulnerability (CVE-2026-0516)
Description	SonicWall has released a security update addressing a vulnerability that exists in their products. **CVE-2026-0516:** An improper neutralization of HTTP Headers for Scripting Syntax vulnerability in SonicOS could allow a remote attacker to manipulate the Host header and redirect firewall management users to arbitrary web domains. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0009

Vendor	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23415, CVE-2026-43450, CVE-2026-43186)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-23415:** A flaw was found in the Linux kernel. A timing issue, known as a race condition, exists within the futex subsystem. This vulnerability could allow a local attacker to access memory after it has been freed, leading to a system crash (denial of service) or potentially the disclosure of sensitive information. **CVE-2026-43450:** A flaw was found in the Linux kernel's nfnetlink_cthelper component. This vulnerability, an out-of-bounds read, occurs in the nfnl_cthelper_dump_table() function when a network connection tracking helper is removed during a dump operation, leading to a bypassed bounds check. A local attacker could exploit this to cause a system crash (denial of service) or potentially access sensitive information from kernel memory. **CVE-2026-43186:** A flaw was found in the Linux kernel's IPv6 In-situ Operations, Administration, and Maintenance (IOAM) functionality. A remote attacker can send a specially crafted packet that manipulates the nodelen field while processing trace data. This manipulation leads to a heap buffer overflow, causing approximately 100 bytes to be written past the allocated memory region. This memory corruption can result in a kernel panic, effectively leading to a Denial of Service (DoS) for 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 9.8 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.8 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.8 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 9.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.8 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.8 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.8 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.8 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.8 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.8 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.8 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.8 s390x Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:51035 • https://access.redhat.com/errata/RHSA-2026:51295

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.