Advisory Alert

Alert Number: AAA20261102 **Date:** November 2, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**Critical**	Use-After-Free Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-49875, CVE-2026-47884, CVE-2026-47890, CVE-2026-84961, CVE-2026-59313, CVE-2026-96760, CVE-2026-90711, CVE-2026-102266, CVE-2026-102267, CVE-2026-102268, CVE-2026-78683, CVE-2026-82617, CVE-2026-13697, CVE-2026-39821, CVE-2026-77413, CVE-2026-47891, CVE-2026-47892, CVE-2026-63374, CVE-2026-59283)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Business Automation versions: • V26.0.0 - V26.0.0-IF003 • V25.0.0 - V25.0.0-IF006 • V24.0.1 - V24.0.1-IF009 • V24.0.0 - V24.0.0-IF010
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7294989

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Use-After-Free Vulnerability (CVE-2026-98432)
Description	Red Hat has released a security update addressing a vulnerability that exists in their products. **CVE-2026-98432:** A flaw was found in the Linux kernel's IPv4 networking subsystem. A race condition occurs during concurrent processing of retransmitted Transmission Control Protocol (TCP) connection requests or socket migrations, allowing socket options to be freed while still in use. A remote attacker could exploit this vulnerability by sending specially timed network requests, triggering a use-after-free condition. This issue primarily results in a system crash leading to a Denial of Service (DoS) or potential memory corruption. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux 8 Base & 8.10 Lifecycle Tiers: RHEL 8 Base: • Base OS: aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder: aarch64, ppc64le, x86_64 RHEL 8.10: • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:93414

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-116443, CVE-2026-116440, CVE-2026-116448, CVE-2026-116449, CVE-2026-116439, CVE-2026-116446, CVE-2026-67271, CVE-2026-116441, CVE-2026-111508, CVE-2026-103813, CVE-2026-111509, CVE-2026-116411, CVE-2026-111545, CVE-2026-107515, CVE-2026-86356, CVE-2026-107524, CVE-2026-82156, CVE-2026-111506, CVE-2026-116447, CVE-2026-107518, CVE-2026-107523, CVE-2026-86355, CVE-2026-111507, CVE-2026-111547, CVE-2026-107519, CVE-2026-116442, CVE-2026-82171, CVE-2026-107516, CVE-2026-107522, CVE-2026-82177, CVE-2026-116413, CVE-2026-116412, CVE-2026-107517, CVE-2026-107520, CVE-2026-107525, CVE-2026-86353, CVE-2026-82179, CVE-2026-107511, CVE-2026-107526, CVE-2026-82174, CVE-2026-82175)
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	PowerStoreT OS verions prior to 5.1.0.0-2798105 used in the below products: • PowerStore 1000T, PowerStore 1200T, PowerStore 1500, PowerStore 3000T, PowerStore 3200Q, PowerStore 3200T, PowerStore 5000T, PowerStore 500T, PowerStore 5200Q, PowerStore 5200T
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000527640/dsa-2026-479-dell-powerstore-t-security-update-for-multiple-vulnerabilities

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22977, CVE-2026-46174, CVE-2026-64191, CVE-2026-68169, CVE-2026-68398, CVE-2026-74283, CVE-2026-80586, CVE-2026-89603, CVE-2026-89932, CVE-2026-90011, CVE-2026-93787, CVE-2026-93827, CVE-2026-98222, CVE-2026-98364, CVE-2026-98432, CVE-2026-98725, CVE-2026-52929, CVE-2026-53228, CVE-2026-53270, CVE-2026-64303, CVE-2026-72083, CVE-2026-74510, CVE-2026-74582, CVE-2026-98466, CVE-2025-68745, CVE-2026-31581, CVE-2026-43493, CVE-2026-46086, CVE-2026-46259, CVE-2026-52972, CVE-2026-63831, CVE-2026-72243, CVE-2026-74641, CVE-2026-89846, CVE-2022-50315, CVE-2026-43020, CVE-2026-43450, CVE-2026-46149, CVE-2026-53224, CVE-2026-53246, CVE-2026-63802, CVE-2026-63920, CVE-2026-63922, CVE-2026-63924, CVE-2026-63984, CVE-2026-63993, CVE-2026-64017, CVE-2026-64319, CVE-2026-72098, CVE-2026-80792)
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 (RHEL):
	RHEL 10 & 10.2:
	• Base OS 10: aarch64, ppc64le, s390x, x86_64
	• CodeReady Linux Builder 10: aarch64, ppc64le, s390x, x86_64
	• Hidden Content 10: x86_64
	• RHEL 10.2 Lifecycle Tiers:
	  ○ Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64
	  ○ CodeReady Linux Builder - Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64
	  ○ 4 Years of Updates / Support: aarch64, ppc64le, s390x, x86_64
	  ○ Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64
	RHEL 9 & Minor Releases:
	• Base OS 9: aarch64, ppc64le, s390x, x86_64
	• CodeReady Linux Builder 9: aarch64, ppc64le, s390x, x86_64
	• RHEL 9.8 Lifecycle Tiers:
	  ○ Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64
	  ○ CodeReady Linux Builder - Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64
	  ○ 4 Years of Updates: aarch64, s390x
	  ○ Update Services for SAP Solutions (E4S): ppc64le, x86_64
	  ○ Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64
	• RHEL 9.2 Lifecycle Tiers:
	  ○ Advanced Update Support (AUS): x86_64
	  ○ Update Services for SAP Solutions (E4S): ppc64le, x86_64
	  ○ 4 Years of Updates: aarch64, s390x
	  ○ Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64
	RHEL 8 Minor Releases:
	• RHEL 8.8 Lifecycle Tiers:
	  ○ Telecommunications Update Service (TUS): x86_64
	  ○ Update Services for SAP Solutions (E4S): ppc64le, x86_64
	  ○ Extended Life Cycle Long Life: x86_64

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:93413 https://access.redhat.com/errata/RHSA-2026:93412 https://access.redhat.com/errata/RHSA-2026:92997 https://access.redhat.com/errata/RHSA-2026:92993

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Cloud Pak for Business Automation versions: • V26.0.0 - V26.0.0-IF003 • V25.0.0 - V25.0.0-IF006 • V24.0.1 - V24.0.1-IF009 • V24.0.0 - V24.0.0-IF010
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7294989

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.