Advisory Alert

Alert Number: AAA20250520 **Date:** May 20, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
HPE	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21208, CVE-2024-10917, CVE-2025-1470, CVE-2025-1471)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause Out-of-bounds Write, NULL Pointer Dereference, Integer Overflow or Wraparound, Observable Discrepancy. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Versions - 10.5.0 - 10.5.11, 11.1.4.0 - 11.1.4.7, 11.5.4.0 - 11.5.9.0, 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7230474

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21966, CVE-2025-21993)
Description	Red Hat has released security updates addressing multiple vulnerabilities in their products. **CVE-2025-21966 -** In the Linux kernel, the following vulnerability has been resolved: dm-flakey: Fix memory corruption in optional corrupt_bio_byte feature Fix memory corruption due to incorrect parameter being passed to bio_init **CVE-2025-21993 -** iscsi_ibft: Fix UBSAN shift-out-of-bounds warning in ibft_attr_show_nic() When performing an iSCSI boot using IPv6, iscsistart still reads the /sys/firmware/ibft/ethernetX/subnet-mask entry. Since the IPv6 prefix length is 64, this causes the shift exponent to become negative, triggering a UBSAN warning. As the concept of a subnet mask does not apply to IPv6, the value is set to ~0 to suppress the warning message. 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 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 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 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:7956

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-28956)
Description	HPE has released a security update addressing an Information Disclosure Vulnerability that exists in Third-party products with intern effect HPE products. **CVE-2024-28956 -** Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.30_01-16-2025 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.30_01-16-2025 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.30_01-16-2025 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.30_01-16-2025 HPE Apollo 2000 Gen10 Plus System - Prior to v2.30_01-16-2025 HPE Apollo 4200 Gen10 Plus System - Prior to v2.30_01-16-2025 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.30_01-16-2025 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.30_01-16-2025 HPE Edgeline e920 Server Blade - Prior to v2.30_01-16-2025 HPE Edgeline e920d Server Blade - Prior to v2.30_01-16-2025 HPE Edgeline e920t Server Blade - Prior to v2.30_01-16-2025 HPE ProLiant DL160 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL180 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL360 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL380 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL560 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL580 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant ML110 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant ML350 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.40_01-16-2025 HPE Synergy 480 Gen10 Compute Module - Prior to v3.40_01-16-2025 HPE Synergy 660 Gen10 Compute Module - Prior to v3.40_01-16-2025 HPE ProLiant XL170r Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant e910 Server Blade - Prior to v3.40_01-16-2025 HPE ProLiant e910t Server Blade - Prior to v3.40_01-16-2025 HPE Apollo 4200 Gen10/HPE ProLiant XL420 Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant XL190r Gen10 Server - Prior to v3.40_01-16-2025 HPE ProLiant DL20 Gen10 Plus server - Prior to v2.30_01_16_2025 HPE ProLiant ML30 Gen10 Plus server - Prior to v2.30_01_16_2025 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.30_01_16_2025 HPE ProLiant DL20 Gen10 Server - Prior to v3.50_01_16_2025 HPE ProLiant ML30 Gen10 Server - Prior to v3.50_01_16_2025 HPE ProLiant MicroServer Gen10 Plus - Prior to v3.50_01_16_2025 HPE ProLiant m750 Server Blade - Prior to v3.50_01_16_2025
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04861en_us&docLocale=en_US

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.