Advisory Alert

Alert Number: AAA20260518 **Date:** May 18, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
MariaDB	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
MongoDB	**Medium**	Stack Exhaustion Vulnerability

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43284, CVE-2026-42945)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-43284**: In the Linux kernel, the following vulnerability has been resolved: xfrm: esp: avoid in-place decrypt on shared skb frags MSG_SPLICE_PAGES can attach pages from a pipe directly to an skb. TCP marks such skbs with SKBFL_SHARED_FRAG after skb_splice_from_iter(), so later paths that may modify packet data can first make a private copy. **CVE-2026-42945**: NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when the rewrite directive is followed by a rewrite, if, or set directive and an unnamed Perl-Compatible Regular Expression (PCRE) capture (for example, $1, $2) with a replacement string that includes a question mark (?). Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 and 10.0 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 and 10.0 s390x • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 and 10.0 ppc64le • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 and 10.0 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0, 9.2, 9.4, 9.6 and 10.0 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2, 9.4 and 9.6 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4, 9.6 and 10.0 aarch64 • Red Hat Enterprise Linux for ARM 64 10 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0, 9.2, 9.4, 9.6 and 10.0 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2, 9.4 and 9.6 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4, 9.6 and 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2, 9.4, 9.6 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4, 9.6 and 10.0 ppc64le • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2, 9.4, 9.6 and 10.0 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4, 9.6 and 10.0 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0, 9.2, 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux Server - AUS 9.2, 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0, 9.2, 9.4 and 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:17795 • https://access.redhat.com/errata/RHSA-2026:17794 • https://access.redhat.com/errata/RHSA-2026:17793 • https://access.redhat.com/errata/RHSA-2026:17791 • https://access.redhat.com/errata/RHSA-2026:17790 • https://access.redhat.com/errata/RHSA-2026:17753 • https://access.redhat.com/errata/RHSA-2026:17752 • https://access.redhat.com/errata/RHSA-2026:17751

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-10744, CVE-2023-42282, CVE-2025-7783, CVE-2026-29063, CVE-2026-27606, CVE-2025-55754, CVE-2025-66614, CVE-2025-62718, CVE-2025-31651, CVE-2025-24813, CVE-2024-56337, CVE-2024-50379, CVE-2026-4800, CVE-2026-33228, CVE-2026-33896, CVE-2026-42044, CVE-2026-42043, CVE-2025-62718, CVE-2026-29063)
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 security fixes at your earliest to protect systems from potential threats.
Affected Products	Cloudera Data Platform Private Cloud Base with IBM (CDP) versions 7.1.9, 7.3.1 and 7.3.2 Platform Navigator in IBM Cloud Pak for Integration (CP4I) versions 16.1.0 to 16.1.0.23 Automation Assets in IBM Cloud Pak for Integration (CP4I) versions 4.0.0-src2 to 4.0.20-sc2 IBM Db2 Big SQL 7.6 on Cloud Pak for Data 4.8 IBM Db2 Big SQL 7.7 on Cloud Pak for Data 5.0 BM Db2 Big SQL 7.8 on Cloud Pak for Data 5.1 IBM Db2 Big SQL 8.2 on Cloud Pak for Data 5.2 IBM Db2 Big SQL 8.3.0, 8.3.1 on Cloud Pak for Data 5.3.0, 5.3.1 up to patch 3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7273162 • https://www.ibm.com/support/pages/node/7273159 • https://www.ibm.com/support/pages/node/7273112 • https://www.ibm.com/support/pages/node/7273152

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31431, CVE-2026-43284, CVE-2026-43500)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-31431**: In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. **CVE-2026-43284**: In the Linux kernel, the following vulnerability has been resolved: xfrm: esp: avoid in-place decrypt on shared skb frags MSG_SPLICE_PAGES can attach pages from a pipe directly to an skb. TCP marks such skbs with SKBFL_SHARED_FRAG after skb_splice_from_iter(), so later paths that may modify packet data can first make a private copy. **CVE-2026-43500**: In the Linux kernel, the following vulnerability has been resolved: rxrpc: Also unshare DATA/RESPONSE packets when paged frags are present The DATA-packet handler in rxrpc_input_call_event() and the RESPONSE handler in rxrpc_verify_response() copy the skb to a linear one before calling into the security ops only when skb_cloned() is true. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Enterprise Sonic Distribution versions prior to 4.5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000465379/dsa-2026-223-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities

Affected Product	**MariaDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44168, CVE-2026-44169, CVE-2026-44170, CVE-2026-44171, CVE-2026-44172, CVE-2026-44173)
Description	MariaDB has released a security update addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. MariaDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MariaDB Community Server Versions 10.6.26, 10.11.17, 11.4.11, 11.8.7 and 12.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/docs/server/security/cve/community-server

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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	Cloudera Data Platform Private Cloud Base with IBM (CDP) versions 7.1.9, 7.3.1 and 7.3.2 Platform Navigator in IBM Cloud Pak for Integration (CP4I) versions 16.1.0 to 16.1.0.23 Automation Assets in IBM Cloud Pak for Integration (CP4I) versions 4.0.0-src2 to 4.0.20-sc2 IBM Db2 Big SQL 7.6 on Cloud Pak for Data 4.8 IBM Db2 Big SQL 7.7 on Cloud Pak for Data 5.0 BM Db2 Big SQL 7.8 on Cloud Pak for Data 5.1 IBM Db2 Big SQL 8.2 on Cloud Pak for Data 5.2 IBM Db2 Big SQL 8.3.0, 8.3.1 on Cloud Pak for Data 5.3.0, 5.3.1 up to patch 3 IBM Content Collector for SAP Applications version 4.0.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7273162 • https://www.ibm.com/support/pages/node/7273159 • https://www.ibm.com/support/pages/node/7270649 • https://www.ibm.com/support/pages/node/7273112 • https://www.ibm.com/support/pages/node/7273150 • https://www.ibm.com/support/pages/node/7273151 • https://www.ibm.com/support/pages/node/7273152 • https://www.ibm.com/support/pages/node/7273156

Affected Product	**MongoDB**
Severity	**Medium**
Affected Vulnerability	Stack Exhaustion Vulnerability (CVE-2026-6811)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-6811**: Stack exhaustion vulnerability in the MongoDB PHP driver can cause application crashes when processing deeply nested BSON documents in unusual circumstances when the source of these BSON documents is not MongoDB Server. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PHP Driver versions 1.21.5 and 2.1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://jira.mongodb.org/browse/PHPC-2636

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.