Advisory Alert

Alert Number: AAA20260911 **Date:** September 11, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
F5	**Critical**	Type Confusion Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42264, CVE-2026-42043, CVE-2026-42044, CVE-2025-62718, CVE-2026-29063, CVE-2026-4800, CVE-2026-45623, CVE-2026-41586)
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 Db2 - Versions 11.5.0 - 11.5.9 IBM Big SQL on IBM Cloud Pak for Data - Version Big SQL 7.7 on Cloud Pak for Data 5.0 IBM Big SQL on IBM Software Hub Version: • Big SQL 7.8 on Software Hub 5.1 • Big SQL 8.2 on Software Hub 5.2 • Big SQL 8.3 on Software Hub 5.3 • Big SQL 8.5 on Software Hub 5.4 up to (including) patch 5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7286976 • https://www.ibm.com/support/pages/node/7286946 • https://www.ibm.com/support/pages/node/7286986

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 Networking OS10 - Versions prior to 10.6.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000507473/dsa-2026-343-security-update-for-dell-networking-os10-vulnerabilities

Vendor	**F5**
Severity	**Critical**
Affected Vulnerability	Type Confusion Vulnerability (CVE-2026-43038)
Description	F5 has released a security update addressing vulnerability that exists in their product. **CVE-2026-43038:** In the Linux kernel: nfsd: fix posix_acl leak on SETACL decode failure nfsaclsvc_decode_setaclargs() and nfs3svc_decode_setaclargs() each call nfs_stream_decode_acl() twice, first for NFS_ACL and then for NFS_DFACL. Each successful call transfers ownership of a freshly allocated posix_acl into argp->acl_access or argp->acl_default. If the first call succeeds but the second fails, the decoder returns false and argp->acl_access is left dangling. ACLPROC2_SETACL.pc_release was wired to nfssvc_release_attrstat and ACLPROC3_SETACL.pc_release was wired to nfs3svc_release_fhandle. Both only call fh_put() and have no knowledge of the ACL fields on argp. The posix_acl_release() pairs sat at the out: labels inside nfsacld_proc_setacl() and nfsd3_proc_setacl(), but svc_process() skips pc_func when pc_decode returns false, so that cleanup is unreachable on decode failure: svc_process_common() pc_decode() /* decode_setaclargs: false */ /* pc_func skipped */ pc_release() /* fh_put only -- ACLs leaked */ The orphaned posix_acl is leaked for the lifetime of the server. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS - Version 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000163277

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68745, CVE-2026-46149, CVE-2026-52942, CVE-2026-52917, CVE-2026-53091, CVE-2026-52986, CVE-2026-53246, CVE-2026-63801, CVE-2026-63971, CVE-2026-64015, CVE-2026-64113, CVE-2026-68376, CVE-2026-68117, CVE-2026-68300, CVE-2026-68315, CVE-2026-74480, CVE-2026-15809, CVE-2026-34986, CVE-2025-5994, CVE-2025-6965, CVE-2025-9566, CVE-2025-49794, CVE-2025-49796, CVE-2025-54518, CVE-2026-1519, CVE-2026-3012, CVE-2026-3039, CVE-2026-5946, CVE-2026-6893, CVE-2026-11331, CVE-2026-13321, CVE-2026-15816, CVE-2026-39821, CVE-2026-43112, CVE-2025-9230, CVE-2026-2340, CVE-2026-3833, CVE-2026-10723, CVE-2026-29111)
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	RHEL 8 (base) — x86_64, s390x, ppc64le, aarch64 RHEL 8 CodeReady Linux Builder — x86_64, ppc64le, aarch64 RHEL 8.10 — Extended Life Cycle (x86_64, ARM64, ppc64le, s390x) RHEL 10 (base) — x86_64, s390x, ppc64le, aarch64 RHEL 10.2 — Extended Update Support (x86_64, s390x, ppc64le, aarch64) RHEL 10.2 — 4 years of updates/support (x86_64, s390x, ppc64le, aarch64) RHEL 10.2 — Extended Life Cycle (x86_64, s390x, ppc64le, aarch64) RHEL 10 CodeReady Linux Builder — x86_64, ppc64le, aarch64, s390x RHEL 10.2 CodeReady Linux Builder — Extended Update Support (x86_64, ppc64le, s390x, aarch64) OpenShift Container Platform 4.16 — RHEL 8 & RHEL 9, all four architectures each (x86_64, ppc64le, s390x, aarch64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:66325 • https://access.redhat.com/errata/RHSA-2026:66355 • https://access.redhat.com/errata/RHSA-2026:62548 • https://access.redhat.com/errata/RHSA-2026:62549

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Real Time Module 15-SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264120-1/

Vendor	**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	IBM Big SQL on IBM Cloud Pak for Data - Version Big SQL 7.7 on Cloud Pak for Data 5.0 IBM QRadar Hub - Versions 1.0.0 - 3.9.0 IBM Big SQL on IBM Software Hub Version: • Big SQL 7.8 on Software Hub 5.1 • Big SQL 8.2 on Software Hub 5.2 • Big SQL 8.3 on Software Hub 5.3 • Big SQL 8.5 on Software Hub 5.4 up to (including) patch 5 IBM Db2 Mirror for i Versions: • 7.4 • 7.5 • 7.6 IBM Db2 Versions: • 11.5.0 - 11.5.9 • 12.1.0 - 12.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7286946 • https://www.ibm.com/support/pages/node/7286970 • https://www.ibm.com/support/pages/node/7286972 • https://www.ibm.com/support/pages/node/7286976 • https://www.ibm.com/support/pages/node/7286981 • https://www.ibm.com/support/pages/node/7286982 • https://www.ibm.com/support/pages/node/7286983 • https://www.ibm.com/support/pages/node/7286985 • https://www.ibm.com/support/pages/node/7286986 • https://www.ibm.com/support/pages/node/7286987 • https://www.ibm.com/support/pages/node/7286990 • https://www.ibm.com/support/pages/node/7286991 • https://www.ibm.com/support/pages/node/7286993 • https://www.ibm.com/support/pages/node/7286998

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.