Advisory Alert

Alert Number: **AAA20251013** **Date:** **October 13, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
F5	**High**	Buffer Overflow Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**Medium**	Security Update
MariaDB	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2025-29481)
Description	F5 has released security updates addressing a Buffer Overflow Vulnerability that exists in third party product which affects Traffix SDC. **CVE-2025-29481** - Buffer Overflow vulnerability in libbpf 1.5.0 allows a local attacker to execute arbitrary code via the bpf_object__init_prog` function of libbpf. Exploitation of this vulnerability could allow an attacker to access sensitive information stored or transmitted by Trafiix SDC. In addition, a successful attack could compromise the integrity of data processed by Trafiix SDC. This vulnerability does not directly cause significant service disruption or denial-of-service conditions under normal circumstances. However, in some advanced exploitation scenarios, attackers may indirectly degrade system performance or partially block functionality. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC v5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000156983

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22555, CVE-2022-50087, CVE-2023-53186, CVE-2025-37823, CVE-2025-37914, CVE-2025-38498)
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 system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 i386 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension (for IBM z Systems) 6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:17734 • https://access.redhat.com/errata/RHSA-2025:17733

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50154, CVE-2024-53168, CVE-2025-21692, CVE-2025-21791, CVE-2025-38477)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP3, 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503539-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503538-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503529-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503528-1/

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-36099)
Description	IBM has released security updates addressing a vulnerability that exists in IBM WebSphere Application Server which affects WebSphere Hybrid Edition. **CVE-2025-36099** - IBM WebSphere Application Server is vulnerable to a denial of service, caused by sending a specially-crafted request. A privileged user could exploit this vulnerability to cause the server to consume memory resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition version 5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7247692

Affected Product	**MariaDB**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52971, CVE-2025-30722, CVE-2025-30693)
Description	MariaDB has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-52971 -** In multiple MariaDB versions, server crashes in JOIN::fix_all_splittings_in_plan. **CVE-2025-30722 -** A vulnerability in the MySQL Client allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Client accessible data as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. **CVE-2025-30693 -** A vulnerability in the MySQL Client allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. MariaDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MariaDB versions 11.4.6, 10.11.12, 10.6.22 and 10.5.29
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/docs/server/security/securing-mariadb/security

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.