# Advisory Alert

**Alert Number:** AAA20260728 **Date:** July 28, 2026

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Vendor | Severity | Vulnerability |
|---|---|---|
| **IBM** | **Critical** | Multiple Vulnerabilities |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Red Hat** | **High** | Multiple Vulnerabilities |
| **F5** | **High**, **Medium** | Multiple Vulnerabilities |
| **IBM** | **High**, **Medium**, **Low** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Vendor | **IBM** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-27459, CVE-2026-33937, CVE-2026-39830, CVE-2026-39831, CVE-2026-39832, CVE-2026-39833, CVE-2026-39834, CVE-2026-42508, CVE-2026-46595, CVE-2026-39821, CVE-2026-2332, CVE-2026-54906, CVE-2026-44024, CVE-2026-33845, CVE-2026-42010, CVE-2026-44930, CVE-2026-42257) |
| 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.<br>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | IBM Cloud Object Storage System 3.8.1.54 - 3.19.5.56<br>IBM Cloud Object Storage System 3.20.0.0 - 3.20.1.59<br>IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions:<br>• v4.8<br>• v5.0<br>• v5.1<br>• v5.2<br>• v5.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7281433<br>https://www.ibm.com/support/pages/node/7281388 |

| | |
|---|---|
| Vendor | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-23240, CVE-2026-31738, CVE-2026-43038, CVE-2026-46113, CVE-2026-53359, CVE-2026-53366) |
| 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 systems.<br>SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | openSUSE Leap 15.5 and 15.6<br>SUSE Linux Enterprise High Performance Computing 15 SP5<br>SUSE Linux Enterprise Live Patching 15-SP5, 15-SP6 and 15-SP7<br>SUSE Linux Enterprise Micro 5.5<br>SUSE Linux Enterprise Real Time 15 SP5, 15 SP6, and 15 SP7<br>SUSE Linux Enterprise Server 15 SP5, 15 SP6 and 15 SP7<br>SUSE Linux Enterprise Server for SAP Applications 15 SP5, 15 SP6 and 15 SP7 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/announcement/2026/suse-su-20263289-1/<br>https://www.suse.com/support/update/announcement/2026/suse-su-20263264-1/<br>https://www.suse.com/support/update/announcement/2026/suse-su-20263256-1/ |

| | |
|---|---|
| Vendor | **Red Hat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-53006, CVE-2026-64600) |
| Description | Red Hat has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2026-53006:** In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in icmpv6_rcv() Caching saddr and daddr before pskb_pull() is problematic since skb->head can change.<br>**CVE-2026-64600:** In the Linux kernel, the following vulnerability has been resolved: xfs: resample the data fork mapping after cycling ILOCK xfs_reflink_fill_{cow_hole,delalloc} are both presented with an inode, a data fork mapping, and a cow fork mapping.<br>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 8 x86_64<br>• Red Hat Enterprise Linux for IBM z Systems 8 s390x<br>• Red Hat Enterprise Linux for Power, little endian 8 ppc64le<br>• Red Hat Enterprise Linux for ARM 64 8 aarch64<br>• Red Hat CodeReady Linux Builder for x86_64 8 x86_64<br>• Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le<br>• Red Hat CodeReady Linux Builder for ARM 64 8 aarch64<br>• Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64<br>• Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64<br>• Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le<br>• Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x<br>• Red Hat Enterprise Linux for x86_64 10 x86_64<br>• Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64<br>• Red Hat Enterprise Linux for Power, little endian 10 ppc64le<br>• Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le<br>• Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le<br>• Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64<br>• Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64<br>• Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2026:47011<br>https://access.redhat.com/errata/RHSA-2026:46951 |

| | |
|---|---|
| Vendor | **F5** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-6478, CVE-2026-6475, CVE-2026-6479) |
| Description | F5 has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2026-6478:** Covert timing channel in comparison of MD5-hashed password in PostgreSQL authentication allows an attacker to recover user credentials sufficient to authenticate. This does not affect scram-sha-256 passwords, the default in all supported releases. However, current databases may have MD5-hashed passwords originating in upgrades from PostgreSQL 13 or earlier.<br>**CVE-2026-6475:** Symlink following in PostgreSQL pg_basebackup plain format and in pg_rewind allows an origin superuser to overwrite local files, e.g. /var/lib/postgres/.bashrc, that hijack the operating system account. It will remain the case that starting the server after these commands implicitly trusts the origin superuser, due to features like shared_preload_libraries.<br>**CVE-2026-6479:** Uncontrolled recursion in PostgreSQL SSL and GSS negotiation allows an attacker able to connect to a PostgreSQL AF_UNIX socket to achieve sustained denial of service. If SSL and GSS are both disabled, an attacker can do the same via access to a PostgreSQL TCP socket.<br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | BIG-IP Next CNF versions:<br>• 2.3.0<br>• 2.0.0 - 2.2.2<br>BIG-IP Next for Kubernetes versions:<br>• 2.3.0<br>• 2.0.0 - 2.2.2<br>BIG-IQ Centralized Management versions:<br>• 8.4.0 - 8.4.2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://my.f5.com/manage/s/article/K000162463<br>https://my.f5.com/manage/s/article/K000162461<br>https://my.f5.com/manage/s/article/K000162429 |

| | |
|---|---|
| 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.<br>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions:<br>• v4.8<br>• v5.0<br>• v5.1<br>• v5.2<br>• v5.3<br>IBM Cloud Object Storage System versions:<br>• 3.8.1.54 - 3.19.5.56<br>• 3.20.0.0 - 3.20.1.59<br>WebSphere Application Server versions 8.5 and 9.0<br>WebSphere Application Server - Liberty versions 17.0.0.3 - 26.0.0.7<br>• IBM Security SOAR versions 51.0.10.1, 51.0.10.0, 51.0.9.2, 51.0.9.1, 51.0.9.0, 51.0.8.2, 51.0.8.1, 51.0.8.0, 51.0.7.2, 51.0.7.1, 51.0.7.0, 51.0.6.2, 51.0.6.1, 51.0.6.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7281384<br>https://www.ibm.com/support/pages/node/7278576<br>https://www.ibm.com/support/pages/node/7281388<br>https://www.ibm.com/support/pages/node/7281433 |

## 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.