Advisory Alert

Alert Number: AAA20260821 **Date:** August 21, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Authentication Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Hitachi	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**	Security Update
MariaDB	**Medium**	Security Update

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-14525)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-14525:** IBM WebSphere Application Server Liberty, which is bundled with IBM Cloud Pak for Applications, is affected by an authentication bypass vulnerability when the rtcomm-1.0 or rtcommGateway-1.0 feature is enabled. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak for Applications versions 5.1, 5.2, 5.3 IBM WebSphere Application Server Liberty versions 17.0.0.3 - 26.0.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7284351

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-10263, CVE-2026-53359, CVE-2025-40026, CVE-2026-14474, CVE-2026-14476, CVE-2026-31790, CVE-2026-43329)
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 systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat OpenShift Container Platform 4.13 x86_64 Red Hat OpenShift Container Platform for Power 4.13 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 s390x Red Hat OpenShift Container Platform for ARM 64 4.13 aarch64 Red Hat OpenShift Container Platform 4.12 x86_64 Red Hat OpenShift Container Platform for Power 4.12 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.12 s390x Red Hat OpenShift Container Platform for ARM 64 4.12 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:54187 https://access.redhat.com/errata/RHSA-2026:54205

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 14.04, 16.04, 18.04, 20.04, 22.04, 24.04, and 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices

Vendor	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-33828, CVE-2026-34335, CVE-2026-40404, CVE-2026-40409, CVE-2026-41092, CVE-2026-41108, CVE-2026-42828, CVE-2026-42836, CVE-2026-42837, CVE-2026-42903, CVE-2026-42904, CVE-2026-42905, CVE-2026-42906, CVE-2026-42907, CVE-2026-42908, CVE-2026-42909, CVE-2026-42911, CVE-2026-42912, CVE-2026-42914, CVE-2026-42915, CVE-2026-42916, CVE-2026-42968, CVE-2026-42969, CVE-2026-42970, CVE-2026-42971, CVE-2026-42972, CVE-2026-42973, CVE-2026-42977, CVE-2026-42978, CVE-2026-42979, CVE-2026-42980, CVE-2026-42983, CVE-2026-42984, CVE-2026-42985, CVE-2026-42986, CVE-2026-42989, CVE-2026-42991, CVE-2026-42992, CVE-2026-42993, CVE-2026-44799, CVE-2026-44801, CVE-2026-44802, CVE-2026-44803, CVE-2026-44812, CVE-2026-44815, CVE-2026-45487, CVE-2026-45586, CVE-2026-45588, CVE-2026-45592, CVE-2026-45593, CVE-2026-45594, CVE-2026-45595, CVE-2026-45596, CVE-2026-45598, CVE-2026-45599, CVE-2026-45601, CVE-2026-45602, CVE-2026-45603, CVE-2026-45605, CVE-2026-45606, CVE-2026-45607, CVE-2026-45608, CVE-2026-45634, CVE-2026-45635, CVE-2026-45636, CVE-2026-45637, CVE-2026-45638, CVE-2026-45639, CVE-2026-45640, CVE-2026-45641, CVE-2026-45642, CVE-2026-45653, CVE-2026-45655, CVE-2026-45656, CVE-2026-45658, CVE-2026-47289, CVE-2026-47291, CVE-2026-47648, CVE-2026-47653, CVE-2026-47656, CVE-2026-48563, CVE-2026-48568, CVE-2026-48570, CVE-2026-48573, CVE-2026-48574, CVE-2026-48575, CVE-2026-48576, CVE-2026-48578, CVE-2026-48583, CVE-2026-49160, CVE-2026-50507, CVE-2026-8863)
Description	Hitachi 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. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform versions: • 5100, 5200, 5500, 5600, 5200H, 5600H, 5100H, 5500H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/06.html

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-20028)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2025-20028:** Time-of-check time-of-use race condition in the WheaERST SMM module for some Intel(R) reference platforms may allow an escalation of privilege. System software adversary with a privileged user combined with a high complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are present without special internal knowledge and requires no user interaction. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS version 2.0.0 (VELOS Systems) F5OS-A versions 1.8.0 to 1.8.3 and 1.5.1 to 1.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162855

Vendor	**MariaDB**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2026-47064)
Description	MariaDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-47064:** Vulnerability in the MySQL Server, MySQL Cluster product of Oracle MySQL (component: Server: Optimizer). Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server, MySQL Cluster. MariaDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MariaDB Enterprise Server versions: • 11.8.8-5 (2026-06-26) • 11.4.12-9 (2026-06-26) • 10.6.27-23 (2026-06-26)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://mariadb.com/docs/server/security/cve/enterprise-server

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.