Advisory Alert

Alert Number: AAA20260701 **Date:** July 1, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31431, CVE-2026-43037, CVE-2026-43284, CVE-2026-46243, CVE-2026-46300, CVE-2026-46333)
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	Red Hat Enterprise Linux for ARM 64 10 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:33486

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-11712, CVE-2026-11708, CVE-2026-12943)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-11712:** IBM WebSphere Application Server is affected by a cross-site scripting vulnerability in the administrative console help system. **CVE-2026-11708:** IBM WebSphere Application Server is affected by a cross-site scripting vulnerability in the administrative console's integrated help system. **CVE-2026-12943:** Management systems in IBM Power environments (HMC and Novalink) could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the system due to improper validation of user supplied input. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WebSphere Application Server - Versions 8.5 & 9.0 PowerVM Novalink Versions • 2.0.0.0 • 2.0.1 • 2.0.2 & 2.0.2.1 • 2.0.3 & 2.0.3.1 • 2.1.0 • 2.1.1 • 2.2.0 • 2.2.1 & 2.2.1.1 • 2.3.0 & 2.3.0.1 • 2.3.1 • 2.3.2 • 2.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7278590 • https://www.ibm.com/support/pages/node/7278666

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46331, CVE-2026-43279, CVE-2026-46090, CVE-2026-46189, CVE-2026-46176, CVE-2026-23216, CVE-2026-45984, CVE-2025-71116, CVE-2026-22984, CVE-2026-22990, CVE-2026-23455, CVE-2026-43125, CVE-2026-43329, CVE-2026-45852, CVE-2026-46227)
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 Enterprise Linux for ARM 64 8 aarch64 & 10 aarch64 Red Hat Enterprise Linux for x86_64 8 x86_64& 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64& x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:33666 • https://access.redhat.com/errata/RHSA-2026:33685 • https://access.redhat.com/errata/RHSA-2026:33743 • https://access.redhat.com/errata/RHSA-2026:33899

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-13759, CVE-2026-13773, CVE-2026-13772, CVE-2026-9006, CVE-2026-11546, CVE-2026-11714, CVE-2026-50645, CVE-2026-9322, CVE-2026-9171, CVE-2024-6119, CVE-2025-55163, CVE-2021-4264, CVE-2025-53864, CVE-2025-48924, CVE-2024-6484, CVE-2024-13009, CVE-2021-23445, CVE-2026-11595)
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	WebSphere Application Server - Versions 8.5 & 9.0 WebSphere Extreme Scale - Versions 8.6.1.0 - 8.6.1.6 WebSphere Application Server Liberty - Versions 17.0.0.3 - 26.0.0.7 IBM Cloud Pak System Versions: • 2.3.4.0 • 2.3.4.1 • 2.3.5.0 • 2.3.3.7 & 2.3.3.7 Ifix1 • 2.3.3.6, 2.3.3.6 Ifix1 & 2.3.3.6 iFix2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7278590 • https://www.ibm.com/support/pages/node/7278595 • https://www.ibm.com/support/pages/node/7278594 • https://www.ibm.com/support/pages/node/7278593 • https://www.ibm.com/support/pages/node/7276600 • https://www.ibm.com/support/pages/node/7278572 • https://www.ibm.com/support/pages/node/7278580 • https://www.ibm.com/support/pages/node/7278576 • https://www.ibm.com/support/pages/node/7277074 • https://www.ibm.com/support/pages/node/7239472

Vendor	**F5**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-61723, CVE-2025-47912, CVE-2025-47907, CVE-2025-58183, CVE-2025-47906, CVE-2025-58189)
Description	F5 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. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP Next SPK Versions: • 2.0.0 - 2.0.2 • 1.7.0 - 1.7.15 • 1.9.0 - 1.9.2 BIG-IP Next CNF Versions: • 2.0.0 - 2.0.2 • 2.1.0 • 1.1.0 - 1.4.0 BIG-IP Next for Kubernetes Versions: • 2.0.0 - 2.1.0 F5OS-A Versions: • 1.8.0 - 1.8.3 • 1.5.1 - 1.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000161990 • https://my.f5.com/manage/s/article/K000161993 • https://my.f5.com/manage/s/article/K000161987 • https://my.f5.com/manage/s/article/K000161988 • https://my.f5.com/manage/s/article/K000161984 • https://my.f5.com/manage/s/article/K000161969

Vendor	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-49501, CVE-2026-40633)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-49501:** Dell PowerScale OneFS versions 9.5.0.0 through 9.10.1.7, and versions 9.11.0.0 through 9.13.0.2 contains an Improper Privilege Management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. **CVE-2026-40633:** Dell PowerScale OneFS versions 9.5.0.0 through 9.10.1.7, versions 9.11.0.0 through 9.13.0.2 contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale Onefs Versions: • 9.5.0.0 through 9.10.1.7 • 9.11.0.0 through 9.13.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000483600/dsa-2026-261-security-update-for-dell-powerscale-onefs-multiple-vulnerabilities

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.