Advisory Alert

Alert Number: AAA20260723 **Date:** July 23, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
NetApp	**High**	Authentication Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Check Point	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34182, CVE-2026-32635)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-34182:** Cryptographic Message Services (CMS) processing fails to perform sufficient input validation on the cipher and tag length fields of AuthEnvelopedData containers. Attackers making use of these vulnerabilities may achieve key-equivalent functionality for a given CMS recipient and/or bypass integrity validation for a given message. **CVE-2026-32635:** Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. A Cross-Site Scripting (XSS) vulnerability has been identified in the Angular runtime and compiler. It occurs when the application uses a security-sensitive attribute (for example href on an anchor tag) together with Angular's ability to internationalize attributes. Enabling internationalization for the sensitive attribute by adding i18n-attribute name bypasses Angular's built-in sanitization mechanism, which when combined with a data binding to untrusted user-generated data can allow an attacker to inject a malicious script. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AIX Versions - 7.2 & 7.3 VIOS Versions - 4.1 IBM Db2 Mirror for i Versions: • 7.4 • 7.5 • 7.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7280621 • https://www.ibm.com/support/pages/node/7280719

Vendor	**NetApp**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-22049)
Description	NetApp has released a security update addressing a vulnerability that exists in their products. **CVE-2026-22049:** ONTAP versions 9.16.1 and higher with WebAuthn multi-factor authentication (MFA) configured are susceptible to a vulnerability related to the Relying Party ID which when successfully exploited could allow an attacker with valid credentials to bypass MFA. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260722-0001

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31488, CVE-2026-31684, CVE-2026-46116, CVE-2026-46209, CVE-2026-46135, CVE-2025-71113, CVE-2026-23110, CVE-2026-46099, CVE-2026-46150, CVE-2026-46215, CVE-2026-53071, CVE-2026-46242, CVE-2026-53362, CVE-2026-53359, CVE-2026-41293, CVE-2026-43514, CVE-2026-43512, CVE-2026-43513, CVE-2026-43515, CVE-2026-42498, CVE-2026-41284, CVE-2026-53404, CVE-2026-55956, CVE-2026-2673)
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 Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.8 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.8 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.8 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.8 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.8 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.8 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.8 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.8 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.8 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.8 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.8 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.8 s390x Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 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 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 Power, little endian - Extended Life Cycle 10.2 ppc64le 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 x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le JBoss Enterprise Web Server Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:43231 • https://access.redhat.com/errata/RHSA-2026:43307 • https://access.redhat.com/errata/RHSA-2026:43826 • https://access.redhat.com/errata/RHSA-2026:44003 • https://access.redhat.com/errata/RHSA-2026:44006 • https://access.redhat.com/errata/RHSA-2026:44007 • https://access.redhat.com/errata/RHSA-2026:43402

Vendor	**Check Point**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16232, CVE-2026-62144, CVE-2026-62145)
Description	Check Point has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-16232:** An unauthenticated attacker can obtain an application login token and use it to login via SmartConsole with full admin privileges and apply changes to the security policy and security configuration. **CVE-2026-62144:** An unauthenticated attacker can run any command on the Management including run-script and exec-command on Security Gateway (Check Point Firewall). **CVE-2026-62145:** A vulnerability in Gaia Portal allows an authenticated attacker with read-only access to run commands as root. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Security Management, Security Management Server, Multi-Domain Security Management Server (MDS) & Security Gateway Versions: • R77.30 • R80 • R80.10 • R80.20 • R80.30 • R81 R81.10 • R81.20 • R82 • R82.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.checkpoint.com/results/sk/sk185169/ • https://support.checkpoint.com/results/sk/sk185152/ • https://support.checkpoint.com/results/sk/sk185153/

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34180, CVE-2026-34182, CVE-2026-42766, CVE-2026-42767, CVE-2026-45445, CVE-2026-45446, CVE-2026-45447, CVE-2026-7383, CVE-2026-9076, CVE-2026-50170, CVE-2026-50171, CVE-2026-54266, CVE-2026-54268, CVE-2026-50557, CVE-2026-54265, CVE-2026-52725, CVE-2026-54267, CVE-2026-27171, CVE-2026-32635, CVE-2026-27970)
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	AIX Versions - 7.2 & 7.3 VIOS Versions - 4.1 IBM Db2 Mirror for i Versions: • 7.4 • 7.5 • 7.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7280621 • https://www.ibm.com/support/pages/node/7280739 • https://www.ibm.com/support/pages/node/7280720 • https://www.ibm.com/support/pages/node/7280719 • https://www.ibm.com/support/pages/node/7280621 • https://www.ibm.com/support/pages/node/7280739

Vendor	**Drupal**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16638, CVE-2026-16640, CVE-2026-16639)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-16638:** The module doesn't sufficiently sanitize the names and descriptions of media items and folders when they are displayed in the media browser, resulting in a stored cross-site scripting (XSS) vulnerability. **CVE-2026-16640:** The module ships with a test script that is accessible to anonymous users and doesn't sufficiently validate user input, leading to a Cross Site Scripting vulnerability. **CVE-2026-16639:** The module doesn't sufficiently validate a short-lived token, allowing an attacker to bypass access control and authenticate as a victim user. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Media Folders Module Versions - prior to 1.0.8 • Search API Autocomplete Module Versions - prior to 1.12.0 • Single Sign-On Module Versions - prior to 1.8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2026-081 • https://www.drupal.org/sa-contrib-2026-082 • https://www.drupal.org/sa-contrib-2026-080

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.