Advisory Alert

Alert Number: AAA20260505 **Date:** May 5, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Progress Software	**Critical**	Authentication Bypass Vulnerability
SUSE	**High**	Security Update
Progress Software	**High**	Improper Input Validation Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Apache HTTP Server	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31789, CVE-2025-66614, CVE-2026-29145, CVE-2026-4800)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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 Storage Defender Copy Data Management – Versions 2.2.0.0 - 2.3.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7271681 • https://www.ibm.com/support/pages/node/7271333

Affected Product	**Progress Software**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-4670)
Description	Progress Software has released a security updates addressing a vulnerability that exists in their product. **CVE-2026-4670:** Authentication bypass by primary weakness vulnerability in Progress Software MOVEit Automation allows Authentication Bypass. This issue affects MOVEit Automation: from 2025.0.0 before 2025.0.9, from 2024.0.0 before 2024.1.8, versions prior to 2024.0.0. Progress Software advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MOVEit Automation – Versions prior to 2025.1.4 MOVEit Automation – Versions prior to 2024.1.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://community.progress.com/s/article/MOVEit-Automation-Critical-Security-Alert-Bulletin-April-2026-CVE-2026-4670-CVE-2026-5174

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2026-31431)
Description	SUSE has released a security update addressing a vulnerability that exists in their product. **CVE-2026-31431:** In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. There is no benefit in operating in-place in algif_aead since the source and destination come from different mappings. Get rid of all the complexity added for in-place operation and just copy the AD directly. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20261671-2/

Affected Product	**Progress Software**
Severity	**High**
Affected Vulnerability	Improper Input Validation Vulnerability (CVE-2026-5174)
Description	Progress Software has released a security update addressing a vulnerabilities that exists in their product. **CVE-2026-5174:** Improper input validation vulnerability in Progress Software MOVEit Automation allows Privilege Escalation. This issue affects MOVEit Automation: from 2025.1.0 before 2025.1.5, from 2025.0.0 before 2025.0.9, from 2024.0.0 before 2024.1.8, versions prior to 2024.0.0. Progress Software advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MOVEit Automation – Versions prior to 2025.1.4 MOVEit Automation – Versions prior to 2024.1.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://community.progress.com/s/article/MOVEit-Automation-Critical-Security-Alert-Bulletin-April-2026-CVE-2026-4670-CVE-2026-5174

ffected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23270, CVE-2026-31402, CVE-2026-31419, CVE-2026-31431, CVE-2026-23136)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in their product. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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 10 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for 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 Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:13566 • https://access.redhat.com/errata/RHSA-2026:13565

Affected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68161, CVE-2025-12635, CVE-2026-34500, CVE-2026-34487, CVE-2026-22796, CVE-2026-31790, CVE-2026-28387, CVE-2026-28388, CVE-2026-28389, CVE-2026-28390, CVE-2026-24733, CVE-2026-24734, CVE-2026-24880, CVE-2026-25854, CVE-2026-29146, CVE-2026-34483, CVE-2026-2950)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise 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 Storage Defender Copy Data Management – Versions 2.2.0.0 - 2.3.0.0 PowerVM Novalink • Version 2.0.0.0, 2.0.1, 2.0.2, 2.0.2.1, 2.0.3, 2.0.3.1 • Version 2.1.0, 2.1.1 • Version 2.2.0, 2.2.1, 2.2.1.1 • Version 2.3.0, 2.3.0.1, 2.3.1, 2.3.2 PowerVM Hypervisor • Version FW1110.00 - FW1110.11 • Version FW1060.00 - FW1060.61 • Version FW950.00 - FW950.G0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7271681 • https://www.ibm.com/support/pages/node/7271507 • https://www.ibm.com/support/pages/node/7271508 • https://www.ibm.com/support/pages/node/7271180 • https://www.ibm.com/support/pages/node/7271333 • https://www.ibm.com/support/pages/node/7271692

Affected Product	**Apache HTTP Server**
Severity	**High,** **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23918, CVE-2026-24072, CVE-2026-28780, CVE-2026-29168, CVE-2026-29169, CVE-2026-33006, CVE-2026-33007, CVE-2026-33523, CVE-2026-33857, CVE-2026-34032, CVE-2026-34059)
Description	ASF has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. ASF advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Apache HTTP Server versions prior to 2.4.67
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

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.