Advisory Alert

Alert Number: AAA20260310 **Date:** March 10, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Stack Buffer Overflow Vulnerability
HP	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Stack Buffer Overflow Vulnerability (CVE-2025-15467)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2025-15467**: Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow. A stack buffer overflow may lead to a crash, causing Denial of Service, or potentially remote code execution. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AIX versions 7.2 and 7.3 VIOS versions 3.1 and 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7262978

Affected Product	**HP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38545, CVE-2025-14180, CVE-2025-14178, CVE-2025-14177, CVE-2025-1735, CVE-2025-6491, CVE-2025-1220, CVE-2025-9230, CVE-2025-9232, CVE-2025-30749, CVE-2025-30754, CVE-2025-30761, CVE-2025-50059, CVE-2025-50106, CVE-2025-53057, CVE-2025-53066, CVE-2025-66200, CVE-2025-65082, CVE-2025-59775, CVE-2025-58098, CVE-2025-55753, CVE-2025-54090, CVE-2025-53020, CVE-2025-49812, CVE-2025-49630, CVE-2025-23048, CVE-2024-47252, CVE-2024-43394, CVE-2024-43204, CVE-2024-42516, CVE-2025-31672, CVE-2025-48734, CVE-2025-12383, CVE-2025-8916, CVE-2025-52434, CVE-2025-52520, CVE-2025-53506, CVE-2025-48989, CVE-2025-55754, CVE-2025-55752, CVE-2025-61795, CVE-2025-59250)
Description	HP has released a security update addressing multiple vulnerabilities that exist in their HP Device Manager product. These vulnerabilities could be exploited by malicious users to compromise the affected systems. HP advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HP Device Manager versions prior to 5.0.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hp.com/us-en/document/ish_14442335-14442364-16/hpsbhf04092

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796, CVE-2025-13333, CVE-2025-14923)
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 and 7.3 VIOS versions 3.1 and 4.1 IBM WebSphere Application version 8.5 and 9.0 IBM WebSphere Hybrid Edition version 5.1 IBM WebSphere Application Server Liberty versions 17.0.0.3 to 26.0.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7262978 • https://www.ibm.com/support/pages/node/7260217 • https://www.ibm.com/support/pages/node/7262950

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38129, CVE-2025-38289, CVE-2025-38349, CVE-2025-38703, CVE-2025-40064, CVE-2025-40168, CVE-2024-47727, CVE-2024-56603, CVE-2025-22056, CVE-2025-38024, CVE-2025-38141)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the Linux Kernel utilized by 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 CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 and 10.0 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 and 10.0 s390x • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 and 10.0 ppc64le • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 and 10.0 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 and 10.0 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 and 10.0 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 and 10.0 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 and 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 and 10.0 ppc64le • Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 and 10.0 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 • Red Hat Enterprise Linux Server - AUS 9.6 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:4111 • https://access.redhat.com/errata/RHSA-2026:4011

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.