Advisory Alert

Alert Number: AAA202604027 **Date:** April 27, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Buffer Overflow Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-1188)
Description	IBM has released a security update addressing a vulnerability that exists in their products. CVE-2026-1188 - In the Eclipse OMR port library component since release 0.2.0, an API function to return the textual names of all supported processor features was not accounting for the separator inserted between processor features. If the output buffer supplied to this function was incorrectly sized, failing to account for the separator when determining when a write to the buffer was safe could lead to a buffer overflow. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	InfoSphere Data Architect versions 9.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7270721

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23191, CVE-2026-23268, CVE-2025-38234, CVE-2025-68818, CVE-2026-23103, CVE-2026-23243, CVE-2026-23272, CVE-2026-23274, CVE-2026-23317, CVE-2025-40309)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• openSUSE Leap 15.4, 15.5, 15.6 • SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5, 15-SP6 • SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 • SUSE Linux Enterprise Server 12 SP5, 15 SP4, 15 SP5 (including LTSS), 15 SP6 • SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4, 15 SP5, 15 SP6 • SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP4, 15 SP5 (including ESPOS and LTSS) • SUSE Linux Enterprise Micro 5.3, 5.4, 5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20261584-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261592-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261606-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261611-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261613-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-61729, CVE-2026-33186)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. CVE-2025-61729 – A remote attacker could exploit this vulnerability by providing a specially crafted certificate during the error string construction process within the HostnameError.Error() function. This flaw, caused by unbounded string concatenation, leads to excessive resource consumption. Successful exploitation can result in a denial of service (DoS) for the affected system. CVE-2026-33186 – A authorization bypass vulnerability, is caused by improper input validation of the HTTP/2 :path pseudo-header. A remote attacker can exploit this by sending raw HTTP/2 frames with a malformed :path that omits the mandatory leading slash. This allows the attacker to bypass defined security policies, potentially leading to unauthorized access to services or information disclosure. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat OpenShift AI
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:10698

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40152, CVE-2023-26048, CVE-2023-26049, CVE-2025-68161, CVE-2021-2163, CVE-2022-3676, CVE-2022-40151, CVE-2023-22045, CVE-2023-22049, CVE-2021-28167, CVE-2022-21541, CVE-2022-21540, CVE-2022-21426, CVE-2021-41041)
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 security fixes at your earliest to protect systems from potential threats.
Affected Products	InfoSphere Data Architect version 9.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7270721

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.