Advisory Alert

Alert Number: AAA20260423 **Date:** April 23, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-15599, CVE-2026-0540, CVE-2026-27601)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their Security SOAR products. **CVE-2025-15599**: DOMPurify 3.1.3 through 3.2.6 and 2.5.3 through 2.5.8 contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting missing textarea rawtext element validation in the SAFE_FOR_XML regex. Attackers can include closing rawtext tags like /textarea in attribute values to break out of rawtext contexts and execute JavaScript when sanitized output is placed inside rawtext elements. **CVE-2026-0540**: DOMPurify 3.1.3 through 3.3.1 and 2.5.3 through 2.5.8, fixed in commit 2726c74, contain a cross-site scripting vulnerability that allows attackers to bypass attribute sanitization by exploiting five missing rawtext elements (noscript, xmp, noembed, noframes, iframe) in the SAFE_FOR_XML regex. Attackers can include payloads like /noscriptimg src=x onerror=alert(1) in attribute values to execute JavaScript when sanitized output is placed inside these unprotected rawtext contexts. **CVE-2026-27601**: Underscore.js is a utility-belt library for JavaScript. Prior to 1.13.8, the _.flatten and _.isEqual functions use recursion without a depth limit. Under very specific conditions, detailed below, an attacker could exploit this in a Denial of Service (DoS) attack by triggering a stack overflow. Untrusted input must be used to create a recursive datastructure, for example using JSON.parse, with no enforced depth limit. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security SOAR versions : • 51.0.9.1 • 51.0.9.0 • 51.0.8.2 • 51.0.8.1 • 51.0.8.0 • 51.0.7.2 • 51.0.7.1 • 51.0.7.0 • 51.0.6.2 • 51.0.6.1 and 51.0.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7270409 • https://www.ibm.com/support/pages/node/7270410

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38024, CVE-2022-50053, CVE-2025-38180, CVE-2023-53539, CVE-2026-23193, CVE-2026-23204, CVE-2026-23216, CVE-2026-23231, CVE-2025-71238, CVE-2026-23001, CVE-2025-38248, CVE-2025-39981, CVE-2025-68800, CVE-2026-23066, CVE-2026-23144, CVE-2026-23171, CVE-2026-23209, CVE-2025-40064, CVE-2025-40168)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise 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 - Extended Life Cycle Support 7 (x86_64, s390x, ppc64, ppc64le) Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0, 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0, 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0, 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0, 9.2 s390x Red Hat Enterprise Linux Server - AUS 8.4, 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:9870 • https://access.redhat.com/errata/RHSA-2026:9836 • https://access.redhat.com/errata/RHSA-2026:9644 • https://access.redhat.com/errata/RHSA-2026:9643

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.