Advisory Alert

Alert Number: AAA20260615 **Date:** June 15, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**Medium**	Cross Site Scripting Vulnerability

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43037, CVE-2024-41073, CVE-2023-53372, CVE-2025-40170, CVE-2025-40135, CVE-2025-40158, CVE-2025-68366, CVE-2025-68724, CVE-2025-71089, CVE-2026-23001, CVE-2026-23216, CVE-2026-31532, CVE-2026-31685, CVE-2026-43038, CVE-2026-43110, CVE-2026-43190)
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 for ARM 64 10 aarch64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 • Red Hat Enterprise Linux Server - AUS 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:25534 https://access.redhat.com/errata/RHSA-2026:25533

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9330, CVE-2026-9311, CVE-2026-8644, CVE-2026-9319)
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	IBM Guardium Key Lifecycle Manager (SKLM/GKLM) version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7276303 https://www.ibm.com/support/pages/node/7276302 https://www.ibm.com/support/pages/node/7276304

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31405, CVE-2026-31629, CVE-2026-31758, CVE-2026-43037, CVE-2026-43206, CVE-2026-43499, CVE-2026-43501, CVE-2026-45852, CVE-2026-45970, CVE-2026-46021, CVE-2026-46043, CVE-2026-46113, CVE-2026-46243)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP4 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262383-1/

Vendor	**IBM**
Severity	**Medium**
Affected Vulnerability	Cross Site Scripting Vulnerability (CVE-2018-1000665)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2018-1000665:** Dojo Dojo Objective Harness (DOH) version prior to version 1.14 contains a Cross Site Scripting (XSS) vulnerability in unit.html and testsDOH/_base/loader/i18n-exhaustive/i18n-test/unit.html and testsDOH/_base/i18nExhaustive.js in the DOH that can result in Victim attacked through their browser - deliver malware, steal HTTP cookies, bypass CORS trust. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Guardium Key Lifecycle Manager versions 4.1, 4.1.1, 4.2, and 4.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7276306

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.