Advisory Alert

Alert Number: AAA20260713 **Date:** July 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-27459)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-27459:** pyOpenSSL is a Python wrapper around the OpenSSL library. Starting in version 22.0.0 and prior to version 26.0.0, if a user provided callback to `set_cookie_generate_callback` returned a cookie value greater than 256 bytes, pyOpenSSL would overflow an OpenSSL provided buffer. Starting in version 26.0.0, cookie values that are too long are now rejected. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	CPDS versions 1.0.0.0 - 1.0.10.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279710

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43074, CVE-2026-46242, CVE-2026-53359, CVE-2026-43499, CVE-2026-53166)
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 Server - AUS 9.4 x86_64 • Red Hat Enterprise Linux for ARM 64 10 aarch64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:37729 https://access.redhat.com/errata/RHSA-2026:37728

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31771, CVE-2026-43038, CVE-2026-46090, CVE-2026-46173, CVE-2026-46229, CVE-2026-46253, CVE-2026-46266, CVE-2026-46274, CVE-2026-46319, CVE-2026-46320, CVE-2026-46331, CVE-2026-52909, CVE-2026-52918, CVE-2026-52923, CVE-2026-52924, CVE-2026-52943, CVE-2026-52955, CVE-2026-52969, CVE-2026-52972, CVE-2026-52993, CVE-2026-53016, CVE-2026-53041, CVE-2026-53053, CVE-2026-53071, CVE-2026-53072, CVE-2026-53133, CVE-2026-53253, CVE-2026-53359, CVE-2026-46197, CVE-2026-46330, CVE-2025-68324, CVE-2026-43198, CVE-2026-45970, CVE-2026-46113)
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Micro 5.3, 5.4 and 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 and 5.4 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262841-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262840-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262839-1/

Vendor	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 18.04 LTS Ubuntu 22.04 LTS Ubuntu 24.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8530-1 https://ubuntu.com/security/notices/USN-8529-1 https://ubuntu.com/security/notices/USN-8528-1 https://ubuntu.com/security/notices/USN-8527-1 https://ubuntu.com/security/notices/USN-8492-5

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-25541, CVE-2026-40895, CVE-2026-34479, CVE-2026-41417, CVE-2026-10535, CVE-2026-10695, CVE-2026-22021, CVE-2026-22013, CVE-2026-22007, CVE-2026-9762, CVE-2026-7771)
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 Fusion versions 2.9.0 - 2.12.2 IBM Fusion HCI versions 2.10.0 - 2.12.2 Content-Aware Storage versions - 1.0.0 - 1.1.4 IBM Db2 Client and Server versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279688 https://www.ibm.com/support/pages/node/7279687 https://www.ibm.com/support/pages/node/7279533 https://www.ibm.com/support/pages/node/7279458 https://www.ibm.com/support/pages/node/7279459 https://www.ibm.com/support/pages/node/7279466 https://www.ibm.com/support/pages/node/7279474 https://www.ibm.com/support/pages/node/7279478 https://www.ibm.com/support/pages/node/7279479 https://www.ibm.com/support/pages/node/7279480

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.