TLP: WHITE

Advisory Alert

Alert Number: AAA20260527 **Date:** May 27, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Joomla	**High**, Medium	Multiple Vulnerabilities
Hitachi	**High**, Medium	Multiple Vulnerabilities
Checkpoint	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21999, CVE-2025-38653, CVE-2025-39766, CVE-2025-68366, CVE-2025-68741, CVE-2026-23243, CVE-2026-23270, CVE-2026-31419, CVE-2026-43163, CVE-2026-24880, CVE-2026-25854, CVE-2026-29145, CVE-2026-29146, CVE-2026-34483, CVE-2026-34487, CVE-2026-34500)
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	JBoss Enterprise Web Server 6 for RHEL 8, 9 and 10 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:21209 • https://access.redhat.com/errata/RHSA-2026:20405 • https://access.redhat.com/errata/RHSA-2026:20406

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50053, CVE-2023-20585, CVE-2024-50082, CVE-2025-68185, CVE-2025-71108, CVE-2025-71118, CVE-2025-71238, CVE-2026-23193, CVE-2026-23209, CVE-2026-23216, CVE-2026-23268, CVE-2026-23269, CVE-2026-23273, CVE-2026-23276, CVE-2026-23290, CVE-2026-23292, CVE-2026-23293, CVE-2026-23312, CVE-2026-23340, CVE-2026-23378, CVE-2026-23391, CVE-2026-23403, CVE-2026-23404, CVE-2026-23405, CVE-2026-23408, CVE-2026-23442, CVE-2026-23449, CVE-2026-23455, CVE-2026-23456, CVE-2026-23457, CVE-2026-23458, CVE-2026-23461, CVE-2026-23462, CVE-2026-23468, CVE-2026-23472, CVE-2026-31393, CVE-2026-31400, CVE-2026-31402, CVE-2026-31403, CVE-2026-31407, CVE-2026-31408, CVE-2026-31411, CVE-2026-31416, CVE-2026-31422, CVE-2026-31423, CVE-2026-31424, CVE-2026-31425, CVE-2026-31427, CVE-2026-31428, CVE-2026-31496, CVE-2026-31504, CVE-2026-31507, CVE-2026-31512, CVE-2026-31524, CVE-2026-31602, CVE-2026-31607, CVE-2026-31649, CVE-2026-31667, CVE-2026-31675, CVE-2026-31681, CVE-2026-31685, CVE-2026-31700, CVE-2026-31738, CVE-2026-31787, CVE-2026-43025, CVE-2026-43088, CVE-2026-43110, CVE-2026-43126, CVE-2026-43190, CVE-2026-43255, CVE-2026-43264, CVE-2026-43334, CVE-2026-43437, CVE-2026-46333)
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	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262068-1/

Affected Product	**Joomla**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48905, CVE-2026-48903, CVE-2026-48902, CVE-2026-48901, CVE-2026-48900, CVE-2026-48899, CVE-2026-48904, CVE-2026-48898, CVE-2026-48897, CVE-2026-48896, CVE-2026-40384, CVE-2026-40383, CVE-2026-35223, CVE-2026-352212, CVE-2026-35221, CVE-2026-35220, CVE-2026-30895, CVE-2026-30894, CVE-2026-25901, CVE-2026-25900)
Description	Joomla 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 Joomla advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Joomla! CMS versions 3.0.0 to 5.4.6 and 6.0.0 to 6.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre.html

Affected Product	**Hitachi**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0390, CVE-2026-20806, CVE-2026-20928, CVE-2026-20930, CVE-2026-23666, CVE-2026-23670, CVE-2026-25250, CVE-2026-26151, CVE-2026-26152, CVE-2026-26153, CVE-2026-26155, CVE-2026-26156, CVE-2026-26159, CVE-2026-26160, CVE-2026-26161, CVE-2026-26162, CVE-2026-26163, CVE-2026-26167, CVE-2026-26168, CVE-2026-26169, CVE-2026-26170, CVE-2026-26172, CVE-2026-26173, CVE-2026-26174, CVE-2026-26175, CVE-2026-26176, CVE-2026-26177, CVE-2026-26178, CVE-2026-26180, CVE-2026-26182, CVE-2026-26184, CVE-2026-27906, CVE-2026-27908, CVE-2026-27909, CVE-2026-27910, CVE-2026-27911, CVE-2026-27914, CVE-2026-27915, CVE-2026-27916, CVE-2026-27917, CVE-2026-27918, CVE-2026-27919, CVE-2026-27920, CVE-2026-27921, CVE-2026-27922, CVE-2026-27923, CVE-2026-27924, CVE-2026-27925, CVE-2026-27926, CVE-2026-27927, CVE-2026-27929, CVE-2026-27930, CVE-2026-27931, CVE-2026-32068, CVE-2026-32069, CVE-2026-32070, CVE-2026-32071, CVE-2026-32072, CVE-2026-32073, CVE-2026-32074, CVE-2026-32075, CVE-2026-32077, CVE-2026-32078, CVE-2026-32079, CVE-2026-32081, CVE-2026-32082, CVE-2026-32083, CVE-2026-32084, CVE-2026-32085, CVE-2026-32086, CVE-2026-32087, CVE-2026-32088, CVE-2026-32089, CVE-2026-32090, CVE-2026-32091, CVE-2026-32093, CVE-2026-32149, CVE-2026-32150, CVE-2026-32151, CVE-2026-32153, CVE-2026-32154, CVE-2026-32155, CVE-2026-32156, CVE-2026-32157, CVE-2026-32158, CVE-2026-32159, CVE-2026-32160, CVE-2026-32162, CVE-2026-32163, CVE-2026-32164, CVE-2026-32165, CVE-2026-32181, CVE-2026-32183, CVE-2026-32202, CVE-2026-32212, CVE-2026-32214, CVE-2026-32215, CVE-2026-32217, CVE-2026-32218, CVE-2026-32225, CVE-2026-32226, CVE-2026-33098, CVE-2026-33099, CVE-2026-33100, CVE-2026-33104, CVE-2026-33116, CVE-2026-33824, CVE-2026-33827, CVE-2026-33829)
Description	Hitachi 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 Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/04.html

Affected Product	**Checkpoint**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48133, CVE-2026-48132, CVE-2026-48131, CVE-2026-48134, CVE-2026-48135, CVE-2026-48136)
Description	Checkpoint 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 Checkpoint advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	R82.10 with Jumbo Hotfix Take 6 or below R82 with Jumbo Hotfix Take 91 or below R81.20 with Jumbo Hotfix Take 127 or below All releases from R81.10 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.checkpoint.com/results/sk/sk184993 • https://support.checkpoint.com/results/sk/sk184982 • https://support.checkpoint.com/results/sk/sk184981 • https://support.checkpoint.com/results/sk/sk184983 • https://support.checkpoint.com/results/sk/sk184991 • https://support.checkpoint.com/results/sk/sk184992

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.