Advisory Alert

Alert Number: AAA20260819 **Date:** August 19, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Zabbix	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Joomla	**Medium**, **Low**	Multiple Vulnerabilities
Apache Struts	**Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14512, CVE-2026-14446, CVE-2026-14529, CVE-2026-2332, CVE-2026-5241)
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 WebSphere Remote Server versions 8.5, 9.0, 9.1 IBM watsonx.data intelligence versions: • 5.2.2, 5.3.0, 5.3.1, 5.4.0, 5.4.0-patch-1 and 5.4.0-patch-2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7284194 https://www.ibm.com/support/pages/node/7284195 https://www.ibm.com/support/pages/node/7284196 https://www.ibm.com/support/pages/node/7284098

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43038, CVE-2026-43125, CVE-2026-43329, CVE-2026-46244, CVE-2026-64530, CVE-2026-23110, CVE-2026-31411, CVE-2026-53016, CVE-2026-53059, CVE-2025-54518, CVE-2026-43112)
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 CodeReady Linux Builder for ARM 64 9.6 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9.6 s390x Red Hat CodeReady Linux Builder for Power, little endian 9.6 ppc64le Red Hat CodeReady Linux Builder for x86_64 9.6 x86_64 Red Hat Enterprise Linux Server 9.4 x86_64 Red Hat Enterprise Linux Server 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE 9.4 ppc64le Red Hat Enterprise Linux Server for Power LE 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 9.6 s390x Red Hat Enterprise Linux for Power, little endian 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 9.6 ppc64le Red Hat Enterprise Linux for x86_64 9.4 x86_64 Red Hat Enterprise Linux for x86_64 9.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:56225 https://access.redhat.com/errata/RHSA-2026:56224 https://access.redhat.com/errata/RHSA-2026:56574 https://access.redhat.com/errata/RHSA-2026:56573

Vendor	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-0980, CVE-2019-0981, CVE-2019-0657, CVE-2025-23299, CVE-2025-23350, CVE-2025-23351, CVE-2023-6237, CVE-2024-4741, CVE-2025-31356, CVE-2022-43680, CVE-2023-52425, CVE-2023-52426, CVE-2024-28757, CVE-2025-59375, CVE-2025-60876, CVE-2025-66382, CVE-2026-24515, CVE-2026-25210, CVE-2026-32776, CVE-2026-32777, CVE-2026-32778, CVE-2026-61407, CVE-2026-32802)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Command Update Software versions prior to 5.7.1 PowerScale Node Firmware Package prior to versions 14.1 in: • PowerScale B100 • PowerScale F200 • PowerScale F210 • PowerScale F600 • PowerScale F710 • PowerScale F900 • PowerScale F910 • PowerScale P100 • PowerScale PA110 Dell PowerPath for Windows Versions 7.2 through to 8.0 SP1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000501378/dsa-2026-309-security-update-for-dell-command-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000501312/dsa-2026-315-security-update-for-dell-powerscale-onefs-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000501078/dsa-2026-248-security-update-for-dell-watchdog-timer-driver-for-an-exposed-ioctl-with-insufficient-access-control-vulnerability • https://www.dell.com/support/kbdoc/en-us/000501417/dsa-2026-167-security-update-for-dell-powerpath-for-windows-vulnerabilities

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14514, CVE-2026-16184, CVE-2026-10842, CVE-2026-14974, CVE-2026-14515, CVE-2026-15328, CVE-2026-14981, CVE-2026-15064, CVE-2026-15325, CVE-2026-14528, CVE-2026-18096, CVE-2026-18097, CVE-2026-16480, CVE-2026-10543, CVE-2026-10534, CVE-2026-45205, CVE-2026-50020, CVE-2026-42578, CVE-2026-50560, CVE-2026-47244, CVE-2026-48043, CVE-2026-45416, CVE-2026-35091, CVE-2026-35092, CVE-2026-57819, CVE-2026-54225, CVE-2026-64958, CVE-2026-48522, CVE-2026-48523, CVE-2026-48524, CVE-2026-48525, CVE-2026-58203, CVE-2026-48710, CVE-2026-54911, CVE-2026-11541, CVE-2026-9071, CVE-2026-53655, CVE-2026-54399, CVE-2026-11525, CVE-2026-12151, CVE-2026-6733, CVE-2026-6734, CVE-2026-9675, CVE-2026-9678, CVE-2026-9679, CVE-2026-9697, CVE-2026-54291, CVE-2026-25087, CVE-2026-8723, CVE-2026-54059, CVE-2026-54060, CVE-2026-55379, CVE-2026-55380, CVE-2026-9320, CVE-2026-8646, CVE-2026-14683, CVE-2026-14684, CVE-2026-14685, CVE-2026-14686, CVE-2026-55760, CVE-2026-11806, CVE-2025-3000, CVE-2026-8149, CVE-2026-44431, CVE-2026-44432, CVE-2026-9375, CVE-2026-44664, CVE-2026-44665, CVE-2024-6763, CVE-2026-54428, CVE-2026-14742, CVE-2026-1839, CVE-2026-48779, CVE-2025-14920, CVE-2026-4372)
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	Reliable Scalable Cluster Technology (RSCT) versions 3.x.x.x IBM WebSphere Remote Server versions 8.5, 9.0 and 9.1 IBM watsonx.data intelligence versions: • 5.2.2, 5.3.0, 5.3.1, 5.4.0, 5.4.0-patch-1 and 5.4.0-patch-2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7283963 https://www.ibm.com/support/pages/node/7284189 https://www.ibm.com/support/pages/node/7284191 https://www.ibm.com/support/pages/node/7284192 https://www.ibm.com/support/pages/node/7284193 https://www.ibm.com/support/pages/node/7284197 https://www.ibm.com/support/pages/node/7284126 https://www.ibm.com/support/pages/node/7284098

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53359, CVE-2026-53228, CVE-2026-53225, CVE-2026-53215, CVE-2026-53212, CVE-2026-53176, CVE-2026-53151, CVE-2026-52931, CVE-2026-52924, CVE-2026-52914, CVE-2026-46331, CVE-2026-46325, CVE-2026-46242, CVE-2026-43465, CVE-2026-43198, CVE-2026-43197, CVE-2026-43083, CVE-2026-53131, CVE-2026-53086, CVE-2026-52989, CVE-2026-46137, CVE-2026-46113, CVE-2026-43499, CVE-2026-43379, CVE-2026-31705, CVE-2026-31636, CVE-2026-31633, CVE-2026-31589, CVE-2026-31501, CVE-2026-31414, CVE-2026-31405, CVE-2026-53260, CVE-2026-53247, CVE-2026-53246, CVE-2026-53224, CVE-2026-53221, CVE-2026-53216, CVE-2026-53186, CVE-2026-53175, CVE-2026-53309, CVE-2026-53043, CVE-2026-53002, CVE-2026-53088, CVE-2026-53045, CVE-2026-53006, CVE-2026-52993, CVE-2026-52986, CVE-2026-52982, CVE-2026-52955, CVE-2026-46266, CVE-2026-43493, CVE-2026-43071, CVE-2026-31668, CVE-2026-31657, CVE-2026-31649, CVE-2026-31448, CVE-2025-27558, CVE-2024-38612, CVE-2021-47378, CVE-2021-47354, CVE-2026-64531)
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 14.04, 16.04, 18.04, 22.04 and 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8630-3 https://ubuntu.com/security/notices/USN-8636-2 https://ubuntu.com/security/notices/USN-8629-3 https://ubuntu.com/security/notices/USN-8646-1 https://ubuntu.com/security/notices/USN-8645-1 https://ubuntu.com/security/notices/USN-8644-1 https://ubuntu.com/security/notices/USN-8643-1

Vendor	**Zabbix**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23922, CVE-2026-23930, CVE-2026-23929, CVE-2026-23931, CVE-2026-23933, CVE-2026-23934, CVE-2026-23935, CVE-2026-23937, CVE-2026-23938, CVE-2026-1199, CVE-2026-59781)
Description	Zabbix 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. Zabbix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Frontend Component versions: • 6.0.0 to 6.0.46 • 7.0.0 to 7.0.27 • 7.4.0 to 7.4.11 Server Component versions: • 6.0.0 to 6.0.46 • 7.0.0 to 7.0.27 • 7.4.0 to 7.4.11 API Component versions: • 6.0.0 to 6.0.46 • 7.0.0 to 7.0.27 • 7.4.0 to 7.4.11 Proxy Component versions: • 6.0.0 to 6.0.46 • 7.0.0 to 7.0.26 • 7.4.0 to 7.4.10 Package Component versions: • 6.0.0 to 6.0.47 • 7.0.0 to 7.0.28 • 7.4.0 to 7.4.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.zabbix.com/browse/ZBX-28067 https://support.zabbix.com/browse/ZBX-28069 https://support.zabbix.com/browse/ZBX-28068 https://support.zabbix.com/browse/ZBX-28070 https://support.zabbix.com/browse/ZBX-28071 https://support.zabbix.com/browse/ZBX-28072 https://support.zabbix.com/browse/ZBX-28073 https://support.zabbix.com/browse/ZBX-28074 https://support.zabbix.com/browse/ZBX-28075 https://support.zabbix.com/browse/ZBX-28076 https://support.zabbix.com/browse/ZBX-28077

Vendor	**Joomla**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-73373, CVE-2026-73372, CVE-2026-73371, CVE-2026-73337, CVE-2026-73336, CVE-2026-72532, CVE-2026-72531, CVE-2026-71574, CVE-2026-71573, CVE-2026-71572)
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 1.0.0-5.4.7, 6.0.0-6.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://developer.joomla.org/security-centre/1077-20260810-core-unrestricted-uploads-of-shtml-files.html • https://developer.joomla.org/security-centre/1076-20260809-core-improper-acl-checks-when-injection-schema-org-contact-data.html • https://developer.joomla.org/security-centre/1075-20260808-core-improper-acl-checks-for-batch-copy-actions.html • https://developer.joomla.org/security-centre/1074-20260807-core-mfa-authentication-bypass.html • https://developer.joomla.org/security-centre/1073-20260806-core-xss-through-schema-org-outputs.html • https://developer.joomla.org/security-centre/1072-20260805-core-improper-acl-checks-for-category-webservice-endpoints.html • https://developer.joomla.org/security-centre/1071-20260804-core-improper-acl-checks-for-custom-fields-webservice-endpoints.html • https://developer.joomla.org/security-centre/1070-20260803-core-inconsistent-acl-checks-for-mutating-webservice-endpoints.html • https://developer.joomla.org/security-centre/1069-20260802-core-improper-cors-origin-validation.html • https://developer.joomla.org/security-centre/1068-20260801-core-response-header-injection-in-download-views.html

Vendor	**Apache Struts**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-73631, CVE-2026-73632, CVE-2026-73633, CVE-2026-73634, CVE-2026-73635)
Description	Apache Struts 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. Apache Struts advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Apache Struts versions: • 2.0.0 through 2.3.37 (EOL) • 2.5.0 through 2.5.33 (EOL) • 6.0.0 through 6.10.0 • 7.0.0 through 7.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://cwiki.apache.org/confluence/spaces/WW/pages/444334417/S2-070 https://cwiki.apache.org/confluence/spaces/WW/pages/444334419/S2-071 https://cwiki.apache.org/confluence/spaces/WW/pages/444334429/S2-072 https://cwiki.apache.org/confluence/spaces/WW/pages/444334431/S2-073 https://cwiki.apache.org/confluence/spaces/WW/pages/444334689/S2-074

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