Advisory Alert

Alert Number: AAA20260507 **Date:** May 7, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
WatchGuard	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Zabbix	**High**, Medium	Multiple Vulnerabilities
Checkpoint	Low	Security Update

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53216, CVE-2025-68741, CVE-2026-23243, CVE-2026-23401, CVE-2026-31431, CVE-2026-31532, CVE-2026-23191, CVE-2026-23193, CVE-2025-71238, CVE-2026-31402, CVE-2025-37861, CVE-2026-23097)
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 - Extended Update Support 9.4 and 9.6 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 and 9.6 s390x • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 and 9.6 ppc64le • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0, 9.4 and 9.6 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 and 9.6 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 and 9.6 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0, 9.4 and 9.6 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 and 9.6 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 and 9.6 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 and 9.6 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 and 9.6 ppc64le • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 and 8.6 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6, 9.0, 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux Server - AUS 8.4, 8.6, 9.4 and 9.6 x86_64 • Red Hat Enterprise Linux Server - TUS 8.6 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6, 9.0, 9.4 and 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:14339 • https://access.redhat.com/errata/RHSA-2026:14230 • https://access.redhat.com/errata/RHSA-2026:14165 • https://access.redhat.com/errata/RHSA-2026:13936 • https://access.redhat.com/errata/RHSA-2026:13932

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6787, CVE-2026-6788, CVE-2026-41288, CVE-2026-41286, CVE-2026-41287)
Description	WatchGuard 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. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	WatchGuard Agent (Windows) version up to and including 1.25.02.0000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00013 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00012 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00011 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00010

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31431, CVE-2025-38375, CVE-2025-39977, CVE-2026-23004, CVE-2026-23204, CVE-2025-71066)
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 15.4 SUSE Linux Enterprise High Performance Computing 12 SP5 and 15 SP4 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4 and 15-SP7 SUSE Linux Enterprise Micro 5.3 and 5.4 SUSE Linux Enterprise Real Time 15 SP4 and SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 and SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 and SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20261724-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261718-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261710-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261708-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261706-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261698-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261694-1/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20172, CVE-2026-20193, CVE-2026-20195, CVE-2026-20189, CVE-2026-20219, CVE-2026-20167, CVE-2026-20168, CVE-2026-20169, CVE-2026-20188, CVE-2026-20185, CVE-2026-20034, CVE-2026-20035)
Description	Cisco 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. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco ECE versions 15, 12 and earlier Cisco ISE versions 3.6, 3.5, 3.4, 3.3, 3.2 and earlier Cisco Prime Infrastructure Release versions 3.10, 3.9 and earlier Cisco IoT Field Network Director Release versions 5, 4 and earlier Cisco CNS 7.2, 7.1 and earlier Cisco NSO 6.5, 6.4, 6.3 and earlier Cisco 350 Series Managed Switches (End of Life) Cisco 350X Series Stackable Managed Switches (End of Life) Cisco Unity Connection versions 15.0, 14.0, 12.5 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-lite-agent-BCgSN8eb#fs • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-bypass-uxjRXGpb • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-unauth-infodiscl-LFnLgmey • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-slido-idor-CpsFmKxN • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iot-fnd-dos-n8N26Q4u • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-dos-7Egqyc • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg350-snmp-dos-GEFZr2Tj • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-rce-ssrf-hENhuASy

Affected Product	**Zabbix**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23928, CVE-2026-23927, CVE-2026-23926)
Description	Zabbix has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-23928**: The Item history widget (in Zabbix 7.0+) or the Plain text widget (in Zabbix 6.0) can execute injected JavaScript when HTML display is enabled. This can allow an attacker to perform unauthorized actions depending on which user opens a dashboard containing these widgets. The malicious JavaScript would have to come from a monitored host controlled by the attacker. **CVE-2026-23927**: A user able to connect to Agent 2 can inject an Oracle TNS connection string via the 'service' parameter. This can lead to Agent 2 connecting to an attacker-controlled server and leaking Oracle database credentials if they are saved in a named session. **CVE-2026-23926**: An authenticated (non-super) administrator can create a maintenance period with a JavaScript payload that is executed by any user that opens tooltip for that maintenance period in the Host navigator widget. This can allow the attacker to perform unauthorized actions depending on which user opens the tooltip. Zabbix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Zabbix Frontend and Agent2 Component versions: • 6.0.0 to 6.0.44 • 7.0.0 to 7.0.23 • 7.4.0 to 7.4.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.zabbix.com/browse/ZBX-27760 • https://support.zabbix.com/browse/ZBX-27759 • https://support.zabbix.com/browse/ZBX-27758

Affected Product	**Checkpoint**
Severity	**Low**
Affected Vulnerability	Security Update (CVE-2026-31431)
Description	Checkpoint has released a security update addressing a vulnerability that exists in their products. **CVE-2026-31431**: In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. There is no benefit in operating in-place in algif_aead since the source and destination come from different mappings. Checkpoint advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Security Gateways versions R82, R82.10 Security Management versions R82, R82.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk184928

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.