



Advisory Alert

Alert Number: AAA20260929

Date: September 29, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	Critical	Multiple Vulnerabilities
WatchGuard	Critical	Multiple Vulnerabilities
Citrix	Critical	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities
WatchGuard	High	OS Command Injection Vulnerability
SUSE	High	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities

Description

Vendor	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-85061, CVE-2026-42044, CVE-2026-42043, CVE-2025-62718, CVE-2026-4800, CVE-2026-29063, CVE-2026-44990, CVE-2026-45623, CVE-2026-42264, CVE-2025-7783)
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	- Use Case Manager App - 1.0.0 - 4.1.1 - IBM QRadar Threat Intelligence - 1.0.0 - 2.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7289781 https://www.ibm.com/support/pages/node/7289777

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaPay Pvt Ltd, 'The Zenith', 161A, Dharmapala Mawatha, Colombo 07, Sri Lanka

Hotline: + 94 112039777

Vendor	WatchGuard
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-86102, CVE-2026-101891)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exist in their products. CVE-2026-86102: An OS command injection vulnerability in the WatchGuard AP internal API service allows an attacker with network access to the AP to execute arbitrary shell commands on the underlying operating system. CVE-2026-101891: An improper access control vulnerability in an internal API service on WatchGuard Access Points allows an unauthenticated attacker with network access to the AP to obtain a valid API session. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard AP Versions: 1.0 - 3.4.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	- https://psirt.watchguard.com/CVE-2026-101891/ - https://psirt.watchguard.com/CVE-2026-86102/

Vendor	Citrix
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-88771, CVE-2026-88772, CVE-2026-88773, CVE-2026-88774, CVE-2026-88775, CVE-2026-88776, CVE-2026-88777, CVE-2026-88778)
Description	Citrix 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. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	- Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1 BEFORE 14.1-73.37 - Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 BEFORE 13.1-64.23 - Citrix NetScaler ADC FIPS BEFORE 14.1-73.37 FIPS - Citrix NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.279
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096&articleURL=Citrix_NetScaler_ADC_and_Citrix_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_88771_CVE_2026_88772_CVE_2026_88773_CVE_2026_88774_CVE_2026_88775_CVE_2026_88776_CVE_2026_88777_and_CVE_2026_88778

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40323, CVE-2026-45942, CVE-2026-46230, CVE-2026-46204, CVE-2026-46199, CVE-2026-63875, CVE-2026-64034, CVE-2026-64556, CVE-2026-68159, CVE-2026-68156, CVE-2026-68155, CVE-2026-68273, CVE-2026-74753, CVE-2026-46325, CVE-2026-52972, CVE-2026-53341, CVE-2026-64102, CVE-2026-80522, CVE-2026-46076, CVE-2026-46317, CVE-2026-68299, CVE-2026-89480, CVE-2026-89775, CVE-2026-45852, CVE-2026-46189, CVE-2026-74581, CVE-2026-46145)
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 Platform & Enterprise Software: Red Hat Enterprise Linux 10 & 10.2: - Base RHEL 10 & CodeReady Linux Builder 10: aarch64, ppc64le, s390x, x86_64 4 Years of Updates / Support: aarch64, ppc64le, s390x, x86_64 - Extended Life Cycle: aarch64, ppc64le, s390x, x86_64 - Extended Update Support (EUS) & CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 Red Hat Enterprise Linux 9 & 9.8: - Base RHEL 9 & CodeReady Linux Builder 9: aarch64, ppc64le, s390x, x86_64 4 Years of Updates: aarch64, s390x - Extended Life Cycle: aarch64, ppc64le, s390x, x86_64 - Extended Update Support (EUS) & CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 - Update Services for SAP Solutions: ppc64le, x86_64 Red Hat Enterprise Linux 8, 8.8 & 8.10: - Base RHEL 8: aarch64, ppc64le, s390x, x86_64 - CodeReady Linux Builder 8: aarch64, ppc64le, x86_64 - Extended Life Cycle (8.10): aarch64, ppc64le, s390x, x86_64 - Extended Life Cycle Long Life (8.8): x86_64 - Update Services for SAP Solutions (8.8): ppc64le, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:72508 https://access.redhat.com/errata/RHSA-2026:72468 https://access.redhat.com/errata/RHSA-2026:72623 https://access.redhat.com/errata/RHSA-2026:72624 https://access.redhat.com/errata/RHSA-2026:72627 https://access.redhat.com/errata/RHSA-2026:72831

Vendor	WatchGuard
Severity	High
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2026-87969)
Description	WatchGuard has released a security update addressing a vulnerability that exists in their products. CVE-2026-87969: An OS command injection vulnerability in the WatchGuard AP diagnostic CLI allows an authenticated administrator to execute arbitrary operating system commands by supplying crafted input. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard AP Versions: 1.0 - 3.4.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-87969/

Vendor	SUSE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities
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	15 SP7 - SUSE Linux Enterprise Server 15 SP7 - SUSE Linux Enterprise Server for SAP Applications 15 SP7 - SUSE Linux Enterprise Live Patching 15-SP7 - SUSE Linux Enterprise Real Time 15 SP7 15 SP6 / Leap 15.6 - openSUSE Leap 15.6 - SUSE Linux Enterprise Server 15 SP6 - SUSE Linux Enterprise Server 15 SP6 LTSS - SUSE Linux Enterprise Server for SAP Applications 15 SP6 - SUSE Linux Enterprise High Availability Extension 15 SP6 - SUSE Linux Enterprise Live Patching 15-SP6 - SUSE Linux Enterprise Real Time 15 SP6 15 SP5 / Leap 15.5 - openSUSE Leap 15.5 - SUSE Linux Enterprise Server 15 SP5 - SUSE Linux Enterprise Server for SAP Applications 15 SP5 - SUSE Linux Enterprise High Performance Computing 15 SP5 - SUSE Linux Enterprise Micro 5.5 - SUSE Linux Enterprise Live Patching 15-SP5 - SUSE Linux Enterprise Real Time 15 SP5 12 SP5 - SUSE Linux Enterprise Server 12 SP5 - SUSE Linux Enterprise Server for SAP Applications 12 SP5 - SUSE Linux Enterprise High Performance Computing 12 SP5 - SUSE Linux Enterprise Live Patching 12-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264356-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264357-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264359-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264360-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264369-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264381-1/

Vendor	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
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	- Use Case Manager App - 1.0.0 - 4.1.1 - IBM QRadar Threat Intelligence - 1.0.0 - 2.5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7289781 https://www.ibm.com/support/pages/node/7289777

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.