Advisory Alert

Alert Number: AAA20261109 **Date:** November 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SonicWall	**High**	Multiple Vulnerabilities
F5	**High**	Infinite Loop Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-111497, CVE-2026-98432, CVE-2025-31936, CVE-2026-12080, CVE-2026-14456, CVE-2026-18798, CVE-2026-19630, CVE-2026-26007, CVE-2026-50252, CVE-2026-52929, CVE-2026-63072, CVE-2026-63076, CVE-2026-64597, CVE-2026-68376, CVE-2026-71226, CVE-2026-77206, CVE-2026-77207, CVE-2026-77214, CVE-2026-80824, CVE-2026-8458, CVE-2026-84782, CVE-2026-8932, CVE-2026-89777, CVE-2026-90003, CVE-2026-90011, CVE-2026-94300, CVE-2026-94453, CVE-2026-96888, CVE-2026-97313, CVE-2026-98222, CVE-2026-98320, CVE-2026-98364, CVE-2026-98466, CVE-2026-98725)
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	OCP 4.19: • RHEL 9: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64) • RHEL 8: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64) OCP 4.20: • RHEL 9: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64) • RHEL 8: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64) OCP 4.21: • RHEL 9: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64) • RHEL 8: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64) OCP 4.22: • RHEL 9: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64) • RHEL 8: x86_64 (Container Platform), ppc64le (for Power), s390x (for IBM Z and LinuxONE), aarch64 (for ARM 64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:95408 • https://access.redhat.com/errata/RHSA-2026:95346 • https://access.redhat.com/errata/RHSA-2026:95523 • https://access.redhat.com/errata/RHSA-2026:95377

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109383, CVE-2026-109829, CVE-2026-90711, CVE-2026-106445, CVE-2026-106446)
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 Versions - 1.0.0 - 4.2.1 IBM QRadar Threat Intelligence Versions - 1.0.0 - 2.6.0 Analyst Workflow Versions - 1.0.0 - 3.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7295909 • https://www.ibm.com/support/pages/node/7295910 • https://www.ibm.com/support/pages/node/7295911

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46195, CVE-2026-52923, CVE-2026-74705, CVE-2026-81000, CVE-2026-103111, CVE-2026-34182, CVE-2026-45445, CVE-2026-59995, CVE-2026-59999, CVE-2026-60002, CVE-2026-86145, CVE-2026-89161, CVE-2026-100655, CVE-2026-100656, CVE-2026-100666, CVE-2026-114488, CVE-2026-12803, CVE-2026-12816, CVE-2026-13506, CVE-2026-14682, CVE-2026-15560, CVE-2026-15564, CVE-2026-17614, CVE-2026-17615, CVE-2026-19610, CVE-2026-19611, CVE-2026-56624, CVE-2026-57819, CVE-2026-58062, CVE-2026-59650, CVE-2026-59651, CVE-2026-59903, CVE-2026-64958, CVE-2026-65432, CVE-2026-65583, CVE-2026-66909, CVE-2026-69152, CVE-2026-75595, CVE-2026-84375, CVE-2026-84725, CVE-2026-85634, CVE-2026-8763, CVE-2026-89058, CVE-2026-89059, CVE-2026-93488, CVE-2026-93491, CVE-2026-93558, CVE-2026-93562, CVE-2026-93565, CVE-2026-93566, CVE-2026-93573, CVE-2026-93574, CVE-2026-92092)
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	RHEL 9 Base: • Base OS: ppc64le, x86_64 RHEL 9.8: • Extended Update Support (EUS): ppc64le, x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • Extended Life Cycle (ELC): ppc64le, x86_64 RHEL 9.6: • Extended Update Support (EUS): ppc64le, x86_64 • Advanced Update Support (AUS): x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • Extended Life Cycle (ELC): ppc64le, x86_64 RHEL 9.4: • Advanced Update Support (AUS): x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • Extended Life Cycle (ELC): ppc64le, x86_64 • Red Hat OpenShift Container Platform 4.16 for RHEL 9: x86_64, ppc64le, s390x, aarch64 • Red Hat OpenShift Container Platform 4.16 for RHEL 8: x86_64, ppc64le, s390x, aarch64 • JBoss Enterprise Application Platform Text-Only Advisories: x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:96090 • https://access.redhat.com/errata/RHSA-2026:96091 • https://access.redhat.com/errata/RHSA-2026:95229 • https://access.redhat.com/errata/RHSA-2026:95887 • https://access.redhat.com/errata/RHSA-2026:95103 • https://access.redhat.com/errata/RHSA-2026:95228 • https://access.redhat.com/errata/RHSA-2026:96093

Vendor	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-107154, CVE-2026-107155, CVE-2026-19703, CVE-2026-19868, CVE-2026-77708, CVE-2026-77709, CVE-2026-82308)
Description	SonicWall 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. SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	7.3.3-7015 and older versions: • Gen7 Hardware Firewalls - TZ 270, TZ 270W, TZ 370, TZ 370W, TZ 470, TZ 470W, TZ 570, TZ 570W, TZ 570P, TZ 670, • NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, • NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 • Gen7 NSv - NSv 270, NSv 470, NSv 870 (ESX, KVM, HYPER-V, AWS, Azure) 8.2.2-8015 and older versions: • Gen8 Hardware Firewalls - TZ 80, TZ 280, TZ 280W, TZ 380, TZ 380W, TZ 480, TZ 580, TZ 680, • NSa 2800, NSa 3800, NSa 4800, NSa 5800 • Gen8 NSv - NSv XS, NSv S, NSv M, NSv L (ESX, KVM, HYPER-V, AWS, Azure)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0014

Vendor	**F5**
Severity	**High**
Affected Vulnerability	Infinite Loop Vulnerability (CVE-2025-8194)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2025-8194:** There is a defect in the CPython “tarfile” module affecting the “TarFile” extraction and entry enumeration APIs. The tar implementation would process tar archives with negative offsets without error, resulting in an infinite loop and deadlock during the parsing of maliciously crafted tar archives. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) Versions: • 17.5.0 - 17.5.1 • 17.1.0 - 17.1.3 BIG-IQ Centralized Management: • 8.4.0 - 8.4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000164129

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 Versions - 1.0.0 - 4.2.1 • IBM QRadar Threat Intelligence Versions - 1.0.0 - 2.6.0 • IBM QRadar Deployment Intelligence App Versions - 1.0.0 - 3.0.20 • QRadar Log Source Management App Versions - 1.0.0 - 7.0.18 • Analyst Workflow Verisons - 1.0.0 - 3.1.1 • IBM Big SQL on Cloud Pak for Data - IBM Big SQL on Cloud Pak for Data 5.0 • IBM Big SQL on Software Hub - IBM Big SQL on Cloud Pak for Data 5.1 • IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.2 • IBM Big SQL on Software Hub - IBM Big SQL on Software Hub 5.3 up to Patch 14 • IBM Storage Defender Copy Data Management Versions - 2.2.0.0 - 2.3.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7295911 • https://www.ibm.com/support/pages/node/7295841 • https://www.ibm.com/support/pages/node/7295286 • https://www.ibm.com/support/pages/node/7295858 • https://www.ibm.com/support/pages/node/7295857 • https://www.ibm.com/support/pages/node/7295910 • https://www.ibm.com/support/pages/node/7295909

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.