Advisory Alert

Alert Number: AAA20260303 **Date:** March 3, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Authorization Bypass Vulnerability
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**	Authentication Bypass Vulnerability
WatchGuard	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Authorization Bypass Vulnerability (CVE-2025-29927)
Description	IBM has released a security update addressing a vulnerability that exists in their QRadar products. **CVE-2025-29927**: It is possible to bypass authorization checks within a Next.js application, if the authorization check occurs in middleware. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar Pre-Validation App versions 2.0.0 - 2.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7262324

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38129, CVE-2023-54142, CVE-2022-50700, CVE-2022-50717, CVE-2021-0920, CVE-2025-38177)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the Linux Kernel utilized by 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, 15.5 and 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 and SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5, 15-SP6 and 15-SP7 SUSE Linux Enterprise Micro 5.3, 5.4 and 5.5 SUSE Linux Enterprise Real Time 15 SP4, SP5, SP6 and SP7 SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4, SP5, SP6 and SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, SP5, SP6 and SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Authorization Bypass Vulnerability (CVE-2026-23600)
Description	HPE has released a security update addressing a vulnerability that exists in their AutoPass License Server products. **CVE-2026-23600**: A potential security vulnerability has been identified in HPE AutoPass License Server (APLS). This vulnerability could be remotely exploited to allow authentication bypass. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE AutoPass License Server - Prior to 9.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn05003en_us&docLocale=en_US

Affected Product	**WatchGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3344, CVE-2026-3343, CVE-2026-3342)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exist in their Firebox products. **CVE-2026-3344**: A vulnerability in WatchGuard Fireware OS may allow an attacker to bypass the Fireware OS filesystem integrity check and maintain limited persistence via a maliciously-crafted firmware update package. **CVE-2026-3343**: A reflected cross-site scripting (XSS) vulnerability in the Fireware OS Web UI enabled execution of malicious JavaScript in the context of an authenticated management user's browser when they click on a specially crafted link. **CVE-2026-3342**: An Out-of-bounds Write vulnerability in WatchGuard Fireware OS may allow an authenticated privileged administrator to execute arbitrary code with root permissions via an exposed management interface. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Fireware OS versions • 11.9 to 11.12.4_Update1 • 12.0 to 12.11.7 • 12.5.9 to 12.5.16 • 2025.1 to 2026.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00005 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00004 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2026-00003

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42446, CVE-2025-30513, CVE-2025-31944, CVE-2025-32007, CVE-2025-32467, CVE-2025-27572, CVE-2025-27940, CVE-2025-22885, CVE-2025-31648, CVE-2026-25907)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their PowerScale 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	PowerScale F210 PowerScale Node Firmware Package Versions prior to 13.2.2 PowerScale F710 PowerScale Node Firmware Package Versions prior to 13.2.2 PowerScale F910 PowerScale Node Firmware Package Versions prior to 13.2.2 PowerScale PA110 PowerScale Node Firmware Package Versions prior to 13.2.2 PowerScale OneFS Version 9.13.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000434554/dsa-2026-100-security-update-for-dell-powerscale-onefs-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000434591/dsa-2026-095-security-update-for-dell-powerscale-onefs-overly-restrictive-account-lockout-mechanism-vulnerability

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-7338, CVE-2025-47935, CVE-2025-48997, CVE-2025-47944, CVE-2025-48387, CVE-2024-12905, CVE-2025-59343, CVE-2025-5889, CVE-2025-32421, CVE-2025-55183, CVE-2025-55184, CVE-2025-67779, CVE-2025-57822, CVE-2024-51479, CVE-2025-55173, CVE-2025-57752, CVE-2025-48068, CVE-2024-56332, CVE-2025-12183, CVE-2025-68161, CVE-2025-66566, CVE-2024-6485, CVE-2025-67735, CVE-2025-59057, CVE-2025-68470, CVE-2026-21884, CVE-2026-22029, CVE-2026-22030, CVE-2025-13466, CVE-2025-14604)
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 QRadar Data Synchronization App versions 1.0.0 to 3.2.0 IBM QRadar Pre-Validation App versions 2.0.0 to 2.0.1 IBM Storage Scale versions 5.2.3.0 - 5.2.3.5 IBM Storage Scale versions 6.0.0.0 - 6.0.0.1 IBM Big SQL 7.7 on Cloud Pak for Data 5.0 IBM Big SQL 7.8 on Cloud Pak for Data 5.1 IBM Big SQL 8.2 on Cloud Pak for Data 5.2 IBM Big SQL 8.3.0 on Cloud Pak for Data 5.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7262325 • https://www.ibm.com/support/pages/node/7262324 • https://www.ibm.com/support/pages/node/7262389 • https://www.ibm.com/support/pages/node/7262121 • https://www.ibm.com/support/pages/node/7262312

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37882, CVE-2025-38106, CVE-2025-38415, CVE-2025-38154, CVE-2025-40168, CVE-2025-71085, 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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:3579 • https://access.redhat.com/errata/RHSA-2026:3520 • https://access.redhat.com/errata/RHSA-2026:3488 • https://access.redhat.com/errata/RHSA-2026:3464

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.