# Advisory Alert

**Alert Number:** AAA20260924 **Date:** September 24, 2026

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Vendor | Severity | Vulnerability |
|---|---|---|
| **Red Hat** | **High** | Multiple Vulnerabilities |
| **WatchGuard** | **High** | Missing / Improper Authentication Vulnerability |
| **Dell** | **High** | Multiple Vulnerabilities |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Drupal** | **High, Medium, Low** | Multiple Vulnerabilities |
| **F5** | **Medium** | Denial of Service (DoS) Vulnerability |
| **IBM** | **Medium, Low** | Multiple Vulnerabilities |

## Description

| Vendor | **Red Hat** |
|---|---|
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-39964, CVE-2026-53266, CVE-2026-23007, CVE-2026-63802, CVE-2026-63831, CVE-2026-64053, CVE-2026-64383, CVE-2026-64564, CVE-2026-68201, CVE-2026-72243, CVE-2026-74569, CVE-2026-80844, CVE-2026-81000, CVE-2026-89846, CVE-2026-53005, CVE-2026-64534, CVE-2026-72261, CVE-2026-43370, CVE-2026-33811, CVE-2026-33818, CVE-2026-39820, CVE-2026-39821, CVE-2026-42499, CVE-2026-42504, CVE-2026-56858, CVE-2026-56859, CVE-2026-56860, CVE-2026-56862, CVE-2026-46150, CVE-2026-52993, CVE-2026-53000, CVE-2026-63887, CVE-2026-63888, CVE-2026-64268) |
| 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.<br><br>Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Red Hat Enterprise Linux & OpenShift Support Matrix:<br><br>OpenShift Container Platform 4.19 (RHEL 8 / 9)<br>Architectures: aarch64, ppc64le, s390x, x86_64<br><br>RHEL 8 Series<br>Base RHEL 8 & CodeReady Linux Builder (aarch64, ppc64le, s390x, x86_64)<br>8.6: AUS (x86_64) \| Extended Life Cycle Long Life (all archs)<br>8.8: Extended Life Cycle Long Life (x86_64) \| TUS (x86_64) \| SAP (ppc64le, x86_64)<br>8.10: Extended Life Cycle (all archs)<br><br>RHEL 9 Series<br>Base RHEL 9 & CodeReady Linux Builder (aarch64, ppc64le, s390x, x86_64)<br>9.2: 4-Year Updates (aarch64, s390x) \| AUS (x86_64) \| ELC (all archs) \| SAP (ppc64le, x86_64)<br>9.6: 4-Year Updates (aarch64, s390x) \| AUS (x86_64) \| ELC / EUS / CRB EUS (all archs) \| SAP (ppc64le, x86_64)<br>9.8: 4-Year Updates (aarch64, s390x) \| ELC / EUS / CRB EUS (all archs) \| SAP (ppc64le, x86_64)<br><br>RHEL 10 Series<br>Base RHEL 10 & CodeReady Linux Builder (aarch64, ppc64le, s390x, x86_64)<br>10.0: 4-Year Updates (all archs) \| EUS / CRB EUS (all archs)<br>10.2: 4-Year Updates (all archs) \| ELC / EUS / CRB EUS (all archs) |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2026:71327<br>https://access.redhat.com/errata/RHSA-2026:71326<br>https://access.redhat.com/errata/RHSA-2026:71325<br>https://access.redhat.com/errata/RHSA-2026:71233<br>https://access.redhat.com/errata/RHSA-2026:71232<br>https://access.redhat.com/errata/RHSA-2026:71213<br>https://access.redhat.com/errata/RHSA-2026:70797<br>https://access.redhat.com/errata/RHSA-2026:68534<br>https://access.redhat.com/errata/RHSA-2026:70482 |

| | |
|---|---|
| Vendor | **WatchGuard** |
| Severity | **High** |
| Affected Vulnerability | Missing / Improper Authentication Vulnerability (CVE-2026-95676) |
| Description | WatchGuard has released a security update addressing a vulnerability that exists in their products.<br>**CVE-2026-95676:** A missing/improper authentication vulnerability in the WatchGuard AuthPoint Gateway's LDAP Sync first-factor authentication allows a remote attacker to bypass single-factor password verification under non-default operating conditions. Additional authentication factors still apply.<br>WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | AuthPoint Authentication Gateway versions:<br>• 4.2.2 to 7.5.0 (>= 4.2.2, < 7.5.1) |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://psirt.watchguard.com/CVE-2026-95676/ |

| | |
|---|---|
| Vendor | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-25275, CVE-2026-25289, CVE-2026-82157, CVE-2026-81455, CVE-2026-31790, CVE-2026-28387, CVE-2026-28388, CVE-2026-28389, CVE-2026-28390, CVE-2026-31789, CVE-2026-82164) |
| 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.<br>Dell 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://www.dell.com/support/kbdoc/en-us/000507012/dsa-2026-412-security-update-for-dell-client-platform-for-multiple-qualcomm-wi-fi-and-bluetooth-driver-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000506503/dsa-2026-404-security-update-for-dell-thinos-10-for-multiple-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000501836/dsa-2026-318-security-update-for-dell-client-platform-for-multiple-openssl-vulnerabilities<br>• https://www.dell.com/support/kbdoc/en-us/000506918/dsa-2026-408-security-update-for-dell-trusted-device-client-for-an-incorrect-permission-assignment-for-critical-resource-vulnerability |

| | |
|---|---|
| Vendor | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-46150, CVE-2026-64423, CVE-2026-64561, CVE-2026-64564, CVE-2026-68138) |
| 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.<br>SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | openSUSE Leap 15.5<br>SUSE Linux Enterprise 12 SP5: High Performance Computing, Live Patching, Server, Server for SAP Applications<br>SUSE Linux Enterprise 15 SP5: High Performance Computing, Live Patching, Real Time, Server, Server for SAP Applications<br>SUSE Linux Enterprise Micro 5.5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/announcement/2026/suse-su-20264312-1/<br>https://www.suse.com/support/update/announcement/2026/suse-su-20264299-1/<br>https://www.suse.com/support/update/announcement/2026/suse-su-20264310-1/ |

| | |
|---|---|
| Vendor | **Drupal** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-96382, CVE-2026-96386, CVE-2026-96380, CVE-2026-96377, CVE-2026-96392, CVE-2026-96391, CVE-2026-96390, CVE-2026-96388, CVE-2026-96387, CVE-2026-96385, CVE-2026-96379, CVE-2026-96384, CVE-2026-96378, CVE-2026-96374, CVE-2026-96376, CVE-2026-96375, CVE-2026-96355, CVE-2026-96356, CVE-2026-96398, CVE-2026-96357, CVE-2026-96364, CVE-2026-96365, CVE-2026-96366, CVE-2026-96373, CVE-2026-96372, CVE-2026-96371, CVE-2026-96369, CVE-2026-96370, CVE-2026-96368, CVE-2026-96367, CVE-2026-96363, CVE-2026-96362, CVE-2026-96359, CVE-2026-96358, CVE-2026-96361, CVE-2026-96360) |
| Description | Drupal 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.<br>Drupal 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://www.drupal.org/security |

| | |
|---|---|
| Vendor | **F5** |
| Severity | **Medium** |
| Affected Vulnerability | Denial of Service (DoS) Vulnerability (CVE-2026-42015) |
| Description | F5 has released a security update addressing a vulnerability that exists in their products.<br>**CVE-2026-42015):** A flaw was found in gnutls. An off-by-one error exists in the PKCS#12 bag element bounds check. This vulnerability allows an remote attacker to write past the internal array of a PKCS#12 bag when appending to a bag that already contains 32 elements. This memory corruption could lead to a denial of service (DoS) or potentially other unspecified impacts.<br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | BIG-IP Next CNF Versions 1.4.0 – 1.4.2<br>BIG-IP Next for Kubernetes Versions 2.2.0 – 2.2.2, and 2.3.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://my.f5.com/manage/s/article/K000163397 |

| | |
|---|---|
| Vendor | **IBM** |
| Severity | **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-11710, CVE-2026-16190, CVE-2026-15887, CVE-2026-15412, CVE-2026-16435, CVE-2026-15396, CVE-2026-15634, CVE-2026-16185, CVE-2026-10841, CVE-2026-11548, CVE-2026-11549, CVE-2026-11722, CVE-2026-9327, CVE-2026-9667, CVE-2026-9338, CVE-2026-16188, CVE-2026-9176, CVE-2026-11540, CVE-2026-11538, CVE-2026-11539, CVE-2026-11711, CVE-2026-16186, CVE-2026-16187, CVE-2026-11537, CVE-2026-16189, CVE-2026-9336, CVE-2026-11545) |
| 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.<br>IBM advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | IBM WebSphere Remote Server 8.5<br>IBM WebSphere Remote Server 8.5, 9.0, 9.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/7289136<br>https://www.ibm.com/support/pages/node/7289134<br>https://www.ibm.com/support/pages/node/7289128 |

## 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.