# Advisory Alert

**Alert Number:** AAA20261106 **Date:** November 6, 2026

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

**Information Classification Level :** TLP: WHITE

## Overview

| Vendor | Severity | Vulnerability |
|---|---|---|
| **Dell** | **Critical** | Multiple Vulnerabilities |
| **Dell** | **High** | Multiple Vulnerabilities |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Red Hat** | **High**, **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Vendor | **Dell** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Dell 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>Dell advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | CloudBoost Virtual Appliance versions prior to 19.14.0.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000529826/dsa-2026-262-security-update-for-dell-cloudboost-virtual-appliance-multiple-vulnerabilities |

| | |
|---|---|
| Vendor | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-4480, CVE-2026-1933, CVE-2026-3012, CVE-2026-4408, CVE-2026-2340, CVE-2026-3238, CVE-2026-27601, CVE-2022-41916, CVE-2022-44640, CVE-2022-42898, CVE-2021-44758, CVE-2022-3116, CVE-2026-39316, CVE-2026-27447, CVE-2026-34979, CVE-2026-34990, CVE-2026-34980, CVE-2026-39314, CVE-2026-41079, CVE-2026-34978, CVE-2026-26996, CVE-2026-27903, CVE-2026-27904, CVE-2026-44432, CVE-2026-44431, CVE-2026-5704, CVE-2025-45582, CVE-2026-23949, CVE-2025-69263, CVE-2025-69264, CVE-2025-69262, CVE-2026-23888, CVE-2026-23889, CVE-2026-23890, CVE-2026-24056, CVE-2026-24131) |
| Description | Dell 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>Dell advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Multiple ThinOS 10 Firmaware versions prior to SecurityAddon_ 2605.10.2616_T10 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000515016/dsa-2026-444-security-update-for-dell-thinos-10-for-multiple-third-party-vulnerabilities |

| | |
|---|---|
| Vendor | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | SUSE 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>SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | SUSE Linux Enterprise High Performance Computing 12 SP5<br>SUSE Linux Enterprise Live Patching 12-SP5<br>SUSE Linux Enterprise Server 12 SP5<br>SUSE Linux Enterprise Server 12 SP5 LTSS<br>SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security<br>SUSE Linux Enterprise Server for SAP Applications 12 SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/announcement/2026/suse-su-20265121-1/ |

| | |
|---|---|
| Vendor | **Red Hat** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2026-84445, CVE-2026-37236, CVE-2025-61726, CVE-2025-61729, CVE-2026-25679, CVE-2026-27136, CVE-2026-27145, CVE-2026-32280, CVE-2026-32283, CVE-2026-33811, CVE-2026-33814, CVE-2026-33818, CVE-2026-39820, CVE-2026-39821, CVE-2026-39822, CVE-2026-42499, CVE-2026-42504, CVE-2026-56853, CVE-2026-56858, CVE-2026-56859, CVE-2026-56860, CVE-2026-56862, CVE-2026-63209, CVE-2026-14199, CVE-2026-15815, CVE-2026-17183, CVE-2026-39834, CVE-2026-42127, CVE-2026-73501, CVE-2026-73502, CVE-2026-76905, CVE-2026-77354, CVE-2026-77405, CVE-2026-77411, CVE-2026-88031, CVE-2026-92542, CVE-2026-92543, CVE-2026-52923, CVE-2026-74705, CVE-2026-81000, CVE-2026-43450, CVE-2026-46056, CVE-2026-46259, CVE-2026-53062, CVE-2026-63920, CVE-2026-63922, CVE-2026-63924, CVE-2026-72243, CVE-2026-99999) |
| 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>Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats. |
| Affected Products | Red Hat OpenShift Container Platform<br>Red Hat OpenShift GitOps<br>OpenShift Compliance Operator<br>Multicluster Global Hub<br>RHEL 9 Minor Releases:<br>• RHEL 9.2 Lifecycle Tiers:<br>  ○ Advanced Update Support (AUS): x86_64<br>  ○ Update Services for SAP Solutions (E4S): ppc64le, x86_64<br>  ○ Extended Life Cycle (ELC): ppc64le, x86_64<br>• RHEL 8 Minor Releases & Base:<br>  ○ RHEL 8 Base: ppc64le, x86_64<br>  ○ RHEL 8.10 Extended Life Cycle (ELC): ppc64le, x86_64<br>• RHEL 8.8 Lifecycle Tiers:<br>  ○ Update Services for SAP Solutions (E4S): ppc64le, x86_64<br>  ○ Extended Life Cycle Long Life: x86_64<br>• RHEL 7 Legacy:<br>  ○ Extended Life Cycle Support (ELS): ppc64 (big endian), ppc64le (little endian), s390x (IBM Z), x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2026:95577<br>https://access.redhat.com/errata/RHSA-2026:95610<br>https://access.redhat.com/errata/RHSA-2026:95612<br>https://access.redhat.com/errata/RHSA-2026:95517<br>https://access.redhat.com/errata/RHSA-2026:95601<br>https://access.redhat.com/errata/RHSA-2026:95556<br>https://access.redhat.com/errata/RHSA-2026:95587<br>https://access.redhat.com/errata/RHSA-2026:95600 |

## 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.