Advisory Alert

Alert Number: AAA20260407 **Date:** April 7, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
F5	**High**	Privilege Escalation Vulnerability
Dell	**High, Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Data Protection Central – Version 19.9 to 19.12 prior to dpc-osupdate-1.1.26-1 PowerProtect DP Series (IDPA) Appliance – Versions prior to 2.7.9 VPlex – Versions prior to 6.2.2.0.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000449107/dsa-2026-173-security-update-for-dell-data-protection-central-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000443350/dsa-2026-124-security-update-for-dell-vplex-multiple-third-party-component-vulnerabilities

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-24303)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2025-24303:** Improper check for unusual or exceptional conditions in the Linux kernel-mode driver for some Intel(R) 800 Series Ethernet before version 1.17.2 may allow an authenticated user to potentially enable escalation of privilege via local access. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	F5OS-A 1.x Versions • 1.8.0 - 1.8.3 • 1.5.1 - 1.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000160637

Affected Product	**Dell**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-27102, CVE-2026-24511, CVE-2026-28261)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-27102**: Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.1.6 and versions 9.11.0.0 through 9.13.0.1, contains an incorrect privilege assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges. **CVE-2026-24511:** Dell PowerScale OneFS, versions 9.5.0.0 through 9.10.1.6 and versions 9.11.0.0 through 9.13.0.0, contains a generation of error message containing sensitive information vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to information disclosure. **CVE-2026-28261:** Dell ObjectScale, versions prior to 4.1.0.3 and version 4.2.0.0, contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to secret exposure. The attacker may be able to use the exposed secret to access the vulnerable system with privileges of the compromised account. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerScale OneFS Versions: • 9.5.0.0 to 9.10.1.6 • 9.11.0.0 to 9.13.0.0 • 9.11.0.0 to 9.13.0.1 ObjectScale Versions: • 4.1.0.3 and prior • 4.2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000449337/dsa-2026-125-security-update-for-dell-powerscale-onefs-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000449325/dsa-2026-143-security-update-for-dell-objectscale-prior-to-4-1-0-3-and-4-2-0-0-insertion-of-sensitive-information-into-log-file-vulnerability

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38109, CVE-2026-23144, CVE-2026-23171, CVE-2026-23209, CVE-2026-23193, CVE-2026-23209, CVE-2026-23204, CVE-2026-23191, CVE-2025-68811)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel of 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 Enterprise Linux for x86_64 10 x86_64, Red Hat Enterprise Linux for IBM z Systems 10 s390x, Red Hat Enterprise Linux for Power, little endian 10 ppc64le, Red Hat Enterprise Linux for ARM 64 10 aarch64, Red Hat CodeReady Linux Builder for x86_64 10 x86_64, Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le, Red Hat CodeReady Linux Builder for ARM 64 10 aarch64, Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x, Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64, Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x, Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le, Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64, Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64, Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le, Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x, Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64, Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64, Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x, Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le, Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:6632 • https://access.redhat.com/errata/RHSA-2026:6692

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.