



Advisory Alert

Alert Number: AAA20260313

Date: March 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Veeam	Critical	Multiple Vulnerabilities
Dell	High	Multiple Vulnerabilities
NetApp	High	Denial of Service Vulnerabilities
Veeam	High	Multiple Vulnerabilities
Red Hat	Medium	Use After Free (UAF) Vulnerability
HPE	Low	Local Escalation of Privilege Vulnerability

Description

Affected Product	Veeam
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-21666, CVE-2026-21667, CVE-2026-21708, CVE-2026-21669, CVE-2026-21671)
Description	Veeam has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Veeam advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Veeam Backup & Replication 13.0.1.1071 and all earlier version 13 builds Veeam Backup & Replication 12.3.2.4165 and all earlier version 12 builds
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none"> https://www.veeam.com/kb4830 https://www.veeam.com/kb4831

Affected Product	Dell
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-7344, CVE-2025-22830)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2024-7344: A UEFI Secure Boot Bypass vulnerability found in the "Reloader" UEFI application. This application is used in several system recovery software suites (such as those from Howyar and Radix). The flaw stems from using a custom PE loader instead of standard secure UEFI functions, allowing an attacker with administrator or root privileges to load unsigned UEFI binaries even when Secure Boot is enabled. CVE-2025-22830: APTIOV contains a vulnerability in BIOS where a skilled user may cause "Race Condition" by local access. A successful exploitation of this vulnerability may lead to resource exhaustion and impact Confidentiality, Integrity, and Availability. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerSwitch Z9664F-ON – Versions prior to 3.54.5.1-11 PowerSwitch E3200-ON Series – Versions prior to v 3.57.5.1-6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none"> https://www.dell.com/support/kbdoc/en-us/000438703/dsa-2026-134-security-update-for-dell-networking-products-for-multiple-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000438711/dsa-2026-135-security-update-for-dell-networking-products-for-multiple-vulnerabilities

Affected Product	NetApp
Severity	High
Affected Vulnerability	Denial of Service Vulnerabilities (CVE-2025-58190, CVE-2025-61726)
Description	NetApp has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2025-58190: Golang versions prior to 0.45.0 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service. CVE-2025-61726: Golang versions prior to 1.24.12 and 1.25.0 prior to 1.25.6 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service. NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Trident Protect
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none"> https://security.netapp.com/advisory/ntap-20260311-0008 https://security.netapp.com/advisory/ntap-20260311-0009

Affected Product	Veeam
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-21668, CVE-2026-21672, CVE-2026-21670)
Description	<p>Veeam has released security updates addressing multiple vulnerabilities that exists in their products.</p> <p>CVE-2026-21672: A High-severity Local Privilege Escalation vulnerability in Windows-based Veeam Backup & Replication servers. It allows a local user with low privileges to elevate their permissions to a higher level, potentially gaining full control over the backup server.</p> <p>CVE-2026-21668: A High-severity File Manipulation vulnerability in Veeam Backup & Replication. This flaw allows an authenticated domain user to bypass existing restrictions and manipulate arbitrary files residing on a Backup Repository.</p> <p>CVE-2026-21670: A High-severity Information Disclosure vulnerability in Veeam Backup & Replication. It allows a low-privileged user to extract saved SSH credentials from the system, which could be used to pivot and access other infrastructure components.</p> <p>Veeam advises to apply these security fixes at your earliest to protect your systems from potential threats.</p>
Affected Products	Veeam Backup & Replication 13.0.1.1071 and all earlier version 13 builds Veeam Backup & Replication 12.3.2.4165 and all earlier version 12 builds
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none"> • https://www.veeam.com/kb4830 • https://www.veeam.com/kb4831

Affected Product	Red Hat
Severity	Medium
Affected Vulnerability	Use After Free (UAF) Vulnerability (CVE-2025-38129)
Description	<p>Red Hat has released a security update addressing a vulnerability that exist in the kernel of their product.</p> <p>CVE-2025-38129: A flaw was found in the Linux kernel. This vulnerability, known as a use-after-free (UAF), occurs in the page_pool_recycle_in_ring function. A local attacker could exploit this by manipulating the system's memory management, causing a freed memory region to be improperly accessed.</p> <p>Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.</p>
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:4444

Affected Product	HPE
Severity	Low
Affected Vulnerability	Local Escalation of Privilege Vulnerability (CVE-2025-31648)
Description	<p>HPE has released a security update addressing a vulnerability that exists in their product.</p> <p>CVE-2025-31648: This firmware-level flaw results from the improper handling of values within the microcode execution flow, specifically during interactions between startup code and System Management Mode (SMM). A local, privileged attacker with specialized internal knowledge of the microcode could exploit this to further escalate their permissions, potentially compromising system confidentiality and integrity.</p> <p>HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.</p>
Affected Products	HPE Compute Scale-up Server 3200 - Prior to v1.70.74
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05024en_us&docLocale=en_US

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.