Advisory Alert

Alert Number: AAA20261013 **Date:** October 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Integer Overflow Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
NetApp	**High**	Security Update
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56171, CVE-2023-4807, CVE-2023-5363, CVE-2024-6119, CVE-2025-70873)
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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SupportAssist SOS Software versions prior to 5.5.16.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000515036/dsa-2026-446-security-update-for-dell-supportassist-os-recovery-for-multiple-third-party-component-vulnerabilities

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Integer Overflow Vulnerability (CVE-2002-0391)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2002-0391:** Integer overflow in xdr_array function in RPC servers for operating systems that use libc, glibc, or other code based on SunRPC including dietlibc, allows remote attackers to execute arbitrary code by passing a large number of arguments to xdr_array through RPC services such as rpc.cmsd and dmispd. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbns05148en_us&docLocale=en_US

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46309, CVE-2026-63925, CVE-2026-64507, CVE-2026-64508, CVE-2026-68123, CVE-2026-68236, CVE-2026-68245, CVE-2026-68278, CVE-2026-72318, CVE-2026-80887, CVE-2026-89811, CVE-2026-89894, CVE-2026-89970, CVE-2026-46181, CVE-2026-64002, CVE-2026-46176, CVE-2026-52933, CVE-2026-43332, CVE-2026-64191, CVE-2026-64385, CVE-2026-72289, CVE-2026-80521, CVE-2026-54099, CVE-2026-54100, CVE-2026-53002, CVE-2026-64007, CVE-2026-74580, CVE-2026-74705)
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	Red Hat Enterprise Linux (RHEL)
	RHEL 10 & 10.2:
	• Base & CodeReady Linux Builder 10 (aarch64, ppc64le, s390x, x86_64)
	• Extended Update Support (EUS) 10.2 (aarch64, ppc64le, s390x, x86_64)
	• CodeReady Linux Builder - Extended Update Support 10.2 (aarch64, ppc64le, s390x, x86_64)
	• 4 Years of Updates / Support 10.2 (aarch64, ppc64le, s390x, x86_64)
	• Extended Life Cycle (ELC) 10.2 (aarch64, ppc64le, s390x, x86_64)
	RHEL 9 Series & Minor Releases:
	• Base & CodeReady Linux Builder 9 (aarch64, ppc64le, s390x, x86_64)
	• RHEL 9.8:
	  ○ Extended Update Support (EUS) & CodeReady Linux Builder EUS (aarch64, ppc64le, s390x, x86_64)
	  ○ 4 Years of Updates (aarch64, s390x)
	  ○ Update Services for SAP Solutions (E4S) (ppc64le, x86_64)
	  ○ Extended Life Cycle (ELC) (aarch64, ppc64le, s390x, x86_64)
	• RHEL 9.6:
	  ○ Advanced Update Support (AUS) (x86_64)
	  ○ Extended Update Support (EUS) (ppc64le, x86_64)
	  ○ Update Services for SAP Solutions (E4S) (ppc64le, x86_64)
	  ○ Extended Life Cycle (ELC) (ppc64le, x86_64)
	• RHEL 9.4:
	  ○ Advanced Update Support (AUS) (x86_64)
	  ○ Update Services for SAP Solutions (E4S) (ppc64le, x86_64)
	  ○ Extended Life Cycle (ELC) (ppc64le, x86_64)
	• RHEL 9.2:
	  ○ Advanced Update Support (AUS) (x86_64)
	  ○ Update Services for SAP Solutions (E4S) (ppc64le, x86_64)
	  ○ Extended Life Cycle (ELC) (ppc64le, x86_64)
	RHEL 8 Series & Minor Releases:
	• Base & CodeReady Linux Builder 8 (ppc64le, x86_64)
	• Extended Life Cycle (ELC) 8.10 (ppc64le, x86_64)
	• Extended Life Cycle Long Life 8.8 (x86_64)
	• Update Services for SAP Solutions (E4S) 8.8 (ppc64le, x86_64)
	RHEL 7 Legacy:
	• Extended Life Cycle Support (ELS) (ppc64, ppc64le, s390x, x86_64)
	Red Hat OpenShift:
	• Red Hat OpenShift for Windows Containers

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:81552 https://access.redhat.com/errata/RHSA-2026:81523 https://access.redhat.com/errata/RHSA-2026:81453 https://access.redhat.com/errata/RHSA-2026:81452 https://access.redhat.com/errata/RHSA-2026:81451 https://access.redhat.com/errata/RHSA-2026:81450 https://access.redhat.com/errata/RHSA-2026:81449 https://access.redhat.com/errata/RHSA-2026:81406 https://access.redhat.com/errata/RHSA-2026:81397 https://access.redhat.com/errata/RHSA-2026:81349

Vendor	**NetApp**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2026-46600)
Description	NetApp has released a security update addressing a vulnerability that exists in their products. **CVE-2026-46600:** Golang.Org/X/Net versions prior to 0.56.0 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp Console Agent Container (tp-proxy) StorageGRID (formerly StorageGRID Webscale) Trident Protect Connector
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20261009-0025

Vendor	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-73790, CVE-2026-73791, CVE-2026-73792, CVE-2026-73793, CVE-2026-73794, CVE-2026-73795, CVE-2026-73796, CVE-2026-73797, CVE-2026-73798, CVE-2026-73799, CVE-2026-76655, CVE-2026-76656, CVE-2026-76659, CVE-2026-76660, CVE-2026-76661, CVE-2026-76662, CVE-2026-76663, CVE-2026-76664, CVE-2026-76665, CVE-2026-76666, CVE-2026-76667, CVE-2026-76668, CVE-2026-79821, CVE-2026-79822, CVE-2026-79823, CVE-2026-79824, CVE-2026-79825, CVE-2026-79826, CVE-2026-79827, CVE-2026-79828, CVE-2026-79829, CVE-2026-79830, CVE-2026-79831, CVE-2026-79832, CVE-2026-79833, CVE-2026-79834, CVE-2026-79835, CVE-2026-79836, CVE-2026-79837, CVE-2026-79838, CVE-2026-79839, CVE-2026-79840, CVE-2026-79841, CVE-2026-79843)
Description	HPE 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. HPE 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://support.hpe.com/hpesc/public/docDisplay?docId=hpesbns05148en_us&docLocale=en_US

Vendor	**Dell**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0893, CVE-2026-82153)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-0893:** Dell Client Platform BIOS remediation is available for an AMI BIOS vulnerability that could be exploited by malicious users to compromise the affected system. **CVE-2026-82153:** Dell OS Recovery Tool, versions prior to 2.4.4, contains an Insecure Storage of Sensitive Information vulnerability. A low privileged attacker with physical access could potentially exploit this vulnerability, leading to Information Disclosure. Dell advises to apply security fixes at your earliest to protect 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/000501823/dsa-2026-229-security-update-for-dell-client-platform-bios-for-an-ami-bios-vulnerability https://www.dell.com/support/kbdoc/en-us/000517461/dsa-2026-450-security-update-for-dell-os-recovery-tool-for-an-insecure-storage-of-sensitive-information-vulnerability

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.