Advisory Alert

Alert Number: AAA20260904 **Date:** September 4, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
SonicWall	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Broadcom	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities

Description

Vendor	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-78327, CVE-2026-78328, CVE-2026-81939)
Description	SonicWall has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-78327:** An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the SonicWall Network Security Manager (NSM) On-Prem Management interface allows an authenticated attacker with SuperAdmin privileges to inject arbitrary commands that are executed on the underlying host, resulting in remote code execution. **CVE-2026-78328:** A missing authorization vulnerability in the SonicWall Network Security Manager (NSM) On-Prem Management interface allows a lower-privileged Admin user to escalate privileges to SuperAdmin. **CVE-2026-81939:** A Zip Slip vulnerability in the SonicWall Network Security Manager (NSM) On-Prem file upload and archive processing functionality allows an attacker to extract files outside the intended destination directory using a specially crafted archive. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SonicWall Network Security Manager (NSM) On-Prem (VMware, Hyper-V, Azure, KVM): v4.3.0 & earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0015

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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Affects the following products that are using SUSE Linux Enterprise 12: • Dell Avamar Data Store Gen4T • Dell Avamar Data Store Gen5A • Dell Avamar Virtual Edition • Dell Avamar Network Data Management Protocol (NDMP) Accelerator • Dell Avamar VMware Image Backup Proxy • Dell Networker Virtual Edition (NVE) • Dell PowerProtect DP Series Appliance (IDPA)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000505510/dsa-2026-313-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-multiple-third-party-vulnerabilities

Vendor	**Broadcom**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-59346, CVE-2026-59347)
Description	Broadcom has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-59346:** VMware Workstation and Fusion contain an integer-overflow vulnerability. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. **CVE-2026-59347:** VMware Workstation and Fusion contain a stack-based buffer-overflow vulnerability in HGFS. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Workstation versions 25H2 & 26H1 VMware Fusion versions 5H2 & 26H1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38288

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11234, CVE-2025-54518, CVE-2026-1933, CVE-2026-2340, CVE-2026-3012, CVE-2026-3833, CVE-2026-4408, CVE-2026-4878, CVE-2026-5260, CVE-2026-5450, CVE-2026-14474, CVE-2026-14476, CVE-2026-28390, CVE-2026-29111, CVE-2026-33845, CVE-2026-33846, CVE-2026-34982, CVE-2026-35177, CVE-2026-41035, CVE-2026-41411, CVE-2026-42009, CVE-2026-42010, CVE-2026-42011, CVE-2026-42013, CVE-2026-43112, CVE-2026-45447, CVE-2026-46483, CVE-2026-48864, CVE-2025-68121, CVE-2026-25679, CVE-2026-32280, CVE-2026-39820, CVE-2026-42499, CVE-2025-5222, CVE-2025-10263, CVE-2025-40026, CVE-2026-1519)
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 OpenShift Container Platform 4.12 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x • Red Hat OpenShift Container Platform 4.17 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:59831 https://access.redhat.com/errata/RHSA-2026:59830 https://access.redhat.com/errata/RHSA-2026:60019

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-49412, CVE-2026-4747, CVE-2026-7270, CVE-2026-39457, CVE-2026-42512, CVE-2026-35414, CVE-2026-45251, CVE-2026-39461, CVE-2026-45259, CVE-2026-45256, CVE-2026-34073, CVE-2026-3446, CVE-2026-24072, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-34180, CVE-2026-34181, CVE-2026-70425, CVE-2026-40635, CVE-2026-46460)
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	Dell PowerScale OneFS: v9.5.0.0 – v9.14.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000505684/dsa-2026-360-security-update-for-dell-powerscale-onefs-multiple-vulnerabilities

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20898, CVE-2026-20715, CVE-2026-20734, CVE-2026-20708, CVE-2026-6726, CVE-2026-6727, CVE-2026-20712, CVE-2026-20885, CVE-2026-20901, CVE-2026-20713)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE StoreEasy 1000 Series & File Controllers - Minimum Required Firmware Versions BIOS Updates: • HPE StoreEasy 1470 (Performance / Storage): Prior to v3.00_08-20-2026 (ROM Families U63, U46) • HPE StoreEasy 1570 (Performance / Storage): Prior to v3.00_08-20-2026 (ROM Families U63, U46) • HPE StoreEasy 1670 (Performance / Storage): Prior to v3.00_08-20-2026 (ROM Families U54, U46) • HPE StoreEasy 1870 (Performance / Storage): Prior to v3.00_08-20-2026 (ROM Families U54, U46, U50) • HPE StoreEasy 1670 Expanded Storage: Prior to v2.70_08-20-2026 (ROM Family U50) • HPE StoreEasy 1660 & 1860 Storage: Prior to v2.70_08-20-2026 (ROM Family U46) & v3.70_08-19-2026 (ROM Family U30) • HPE StoreEasy 1460, 1560, 1660 Expanded, 1660 Performance, 1860 Performance & HPE Storage File Controllers (Standard / Performance): Prior to v3.70_08-19-2026 (ROM Families U30, U32, U33, U39) SPS Updates: • HPE StoreEasy 1670 Expanded Storage: Prior to SPS_E5_04.04.04.926.0 (ROM Family U50) • HPE StoreEasy 1660 & 1860 Storage: Prior to SPS_E5_04.04.04.926.0 (ROM Family U46) & SPS_E5_04.01.05.312.0 / SPS 04.01.05.201 (ROM Family U30) • HPE StoreEasy 1460, 1560, 1660 Expanded, 1660 Performance, 1860 Performance & HPE Storage File Controllers (Standard / Performance): Prior to SPS_E5_04.01.05.312.0 / SPS 04.01.05.201 (ROM Families U30, U32, U33, U39)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05143en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05110en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05094en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05095en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05109en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05108en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05120en_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.