Advisory Alert

Alert Number: AAA20250731 **Date:** July 31, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Security Update
Dell	**High**	Multiple Vulnerabilities
RedHat	**High**, **Medium**	Multiple Vulnerabilities
Broadcom VMware	**Medium**	Denial-of-Service Vulnerability
SonicWall	**Medium**	Use of Externally-Controlled Format String Vulnerability

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-54085)
Description	NetApp has released a security update addressing a vulnerability that exists in their product. Successful exploitation of this vulnerability could lead to the disclosure of sensitive information, addition or modification of data, or a denial-of-service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	StorageGRID Baseboard Management Controller (BMC) - SG6160/SGF6112/SG110/SG1100
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250328-0003

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28746, CVE-2023-32282, CVE-2023-22655)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their product. These vulnerabilities could be exploited by malicious users to cause information disclosure and potentially enable privilege escalation via local access. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerSwitch Z9664F-ON – Versions prior to 3.54.5.1-9 PowerSwitch Z9432F-ON – Versions prior to 3.51.5.1-21 PowerSwitch Z9264F-ON – Versions prior to 3.42.5.1-21 PowerSwitch S5448F-ON – Versions prior to 3.52.5.1-12 PowerSwitch E3200-ON Series – Versions prior to 3.57.5.1-5 PowerSwitch N2200-ON Series – Versions prior to 3.45.5.1-31 PowerSwitch N3200-ON Series – Versions prior to 3.45.5.1-31 Dell EMC Networking VEP1425 / VEP1445 / VEP1485 – BIOS versions prior to 2.6 Dell SD-WAN EDGE620 / EDGE640 / EDGE680 – BIOS versions prior to 3.50.0.9-21 Dell SD-WAN EDGE610 / EDGE610-LTE – BIOS versions prior to 3.43.0.9-24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000321646/dsa-2025-197-security-update-for-dell-networking-products-for-multiple-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-57980, CVE-2025-21759, CVE-2025-21905, CVE-2025-22113, CVE-2025-37958, CVE-2025-38001, CVE-2025-38052, CVE-2022-49058, CVE-2022-50022, CVE-2025-22004, CVE-2025-37738, CVE-2025-48976, CVE-2025-48988, CVE-2025-49125, CVE-2025-53506)
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 affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 9.2 x86_64, AUS 8.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 JBoss Enterprise Web Server 6 for RHEL 8 x86_64, 9 x86_64, 10 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:12209 • https://access.redhat.com/errata/RHSA-2025:12238 • https://access.redhat.com/errata/RHSA-2025:11742 • https://access.redhat.com/errata/RHSA-2025:11741

Affected Product	**Broadcom VMware**
Severity	**Medium**
Affected Vulnerability	Denial-Of-Service Vulnerability (CVE-2025-41241)
Description	Broadcom has released security updates addressing a denial-of-service vulnerability that exist in VMware products. **CVE-2025-41241-** A malicious actor who is authenticated through vCenter and has permission to perform API calls for guest OS customisation may trigger this vulnerability to create a denial-of-service condition. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware vCenter 8.0 , 7.0 VMware Cloud Foundation 5.x , 4.5.x, VMware Telco Cloud Platform vCenter 5.x, 2.x VMware Telco Cloud Infrastructure 2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35964

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Use of Externally-Controlled Format String Vulnerability (CVE-2025-40600)
Description	SonicWall has released security updates addressing a Use of Externally-Controlled Format String vulnerability in the SonicOS SSL VPN interface. This Vulnerability allows a remote, unauthenticated attacker to cause service disruption. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following products which are running on SonicOS 7.2.0-7015 and older versions • Gen7 hardware Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W,TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 • Gen7 virtual Firewalls (NSv) - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0013

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.