Advisory Alert

Alert Number: AAA20250616 **Date:** June 16, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Multiple Vulnerabilities
Sonicwall	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
NetApp	**High, Medium**	Multiple Vulnerabilities
HPE	**Medium**	Remote authentication bypass Vulnerability

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45341, CVE-2024-47685)
Description	NetApp has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2024-45341** - A certificate validation vulnerability in Go's crypto/x509 package, which under specific conditions could allow an attacker to bypass URI name constraints using IPv6 addresses with zone identifiers. **CVE-2024-47685** - A vulnerability in the Linux kernel's Netfilter IPv6 TCP reset handling, which in specific cases could result in leaking uninitialized memory through improperly constructed TCP headers. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere Data Infrastructure Insights Telegraf Agent (formerly Cloud Insights Telegraf Agent) E-Series SANtricity OS Controller Software 11.x NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S/ H410C/ H610C/ H610S/ H615C NetApp HCI Compute Node (Bootstrap OS) NetApp Kubernetes Monitoring Operator NetApp SolidFire & HCI Management Node NetApp SolidFire & HCI Storage Node (Element Software) OnCommand Workflow Automation ONTAP 9 ONTAP Select Deploy administration utility Trident
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250221-0004 • https://security.netapp.com/advisory/ntap-20250613-0011

Affected Product	**Sonicwall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38475, CVE-2024-40763, CVE-2024-45318, CVE-2024-45319, CVE-2024-53702, CVE-2024-53703)
Description	SonicWall has released a security update addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to buffer overflows, unauthenticated remote code execution, or unauthorized access. Sonicwall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SMA 100 Series (SMA 200, 210, 400, 410, 500v) - versions 10.2.1.13-72sv and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0018

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24311, CVE-2025-25215, CVE-2025-24922, CVE-2025-25050, CVE-2025-24919)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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/000276106/dsa-2025-053

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3/15.4/15.6 SUSE Linux Enterprise High Performance Computing 15 SP3/15 SP4 SUSE Linux Enterprise Live Patching 15-SP3/15-SP4/15-SP6 SUSE Linux Enterprise Micro 5.1/5.2/5.3/5.4 SUSE Linux Enterprise Real Time 15 SP4/15 SP6 SUSE Linux Enterprise Server 15 SP3/15 SP4/15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP3/15 SP4/15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202501958-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501957-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501956-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501951-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501950-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501949-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501948-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501944-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501932-1/

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	NetApp 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. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere Active IQ Unified Manager for Microsoft Windows Astra Control Center - NetApp Kubernetes Monitoring Operator Data Infrastructure Insights Telegraf Agent (formerly Cloud Insights Telegraf Agent) NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S/ H410C/ H610C/ H610S/ H615C NetApp HCI Compute Node (Bootstrap OS) NetApp Manageability SDK NetApp SolidFire & HCI Management Node NetApp SolidFire & HCI Storage Node (Element Software) ONTAP 9 ONTAP tools for VMware vSphere 9/10 ONTAP Select Deploy administration utility OnCommand Workflow Automation SAN Host Utilities for Windows Trident E-Series SANtricity OS Controller Software 11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250321-0006 • https://security.netapp.com/advisory/ntap-20240926-0003 • https://security.netapp.com/advisory/ntap-20250306-0004 • https://security.netapp.com/advisory/ntap-20250523-0010 • https://security.netapp.com/advisory/ntap-20250613-0009 • https://security.netapp.com/advisory/ntap-20250613-0012 • https://security.netapp.com/advisory/ntap-20250613-0010 • https://security.netapp.com/advisory/ntap-20250328-0009 • https://security.netapp.com/advisory/ntap-20250328-0009 • https://security.netapp.com/advisory/ntap-20250328-0010 • https://security.netapp.com/advisory/ntap-20221118-0007 • https://security.netapp.com/advisory/ntap-20250221-0003 • https://security.netapp.com/advisory/ntap-20241018-0006

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Remote authentication bypass Vulnerability (CVE-2024-54009)
Description	HPE has released a security update addressing a Remote authentication bypass Vulnerability that exists in their products. **CVE-2024-54009 -** Remote authentication bypass vulnerability in HPE Alletra Storage MP B10000 in versions prior to version 10.4.5 could be remotely exploited to allow disclosure of information. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE GreenLake for Block Storage OS - Prior to 10.4.8 HPE Alletra 9000 - Prior to 9.6.3 - Operating System HPE 3PAR Operating System Software - Prior to 3.3.2 EMU1 P20 HPE Primera 600 Storage - Prior to 4.6.3 - Operating System
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04822en_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.