Advisory Alert

Alert Number: AAA20251120 **Date:** November 20, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Multiple Vulnerabilities
SonicWall	**High**	Multiple Vulnerabilities
NetApp	**High**	Security Update
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-49794, CVE-2025-49796)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in Libxml2 which is incorporated within their products. **CVE-2025-49794, CVE-2025-49796:** Libxml2 versions through 2.14.4 are susceptible to a vulnerability which when successfully exploited could lead to addition or modification of data or Denial of Service (DoS). NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetApp Manageability SDK
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250718-0003 • https://security.netapp.com/advisory/ntap-20250718-0004

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40604, CVE-2025-40605, CVE-2025-40601)
Description	SonicWall has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-40604**: Download of Code Without Integrity Check Vulnerability in the SonicWall Email Security appliance loads root filesystem images without verifying signatures, allowing attackers with VMDK or datastore access to modify system files and gain persistent arbitrary code execution. **CVE-2025-40605**: A Path Traversal vulnerability has been identified in the Email Security appliance allows an attacker to manipulate file system paths by injecting crafted directory-traversal sequences (such as ../) and may access files and directories outside the intended restricted path. **CVE-2025-40601**: A Stack-based buffer overflow vulnerability in the SonicOS SSLVPN service allows a remote unauthenticated attacker to cause Denial of Service (DoS), which could cause an impacted firewall to crash SonicWall advises to apply this security fixes at your earliest to protect your systems from potential threats.
Affected Products	• ES Appliance 5000, 5050, 7000, 7050, 9000, VMWare and Hyper-V versions 10.0.33.8195 and earlier. • 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 versions 7.3.0-7012 and older. • Gen7 virtual Firewalls (NSv) - NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure) versions 7.3.0-7012 and older. • Gen8 Firewalls - TZ80, TZ280, TZ380, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800 versions 8.0.2-8011 and older.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0018 • https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0016

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-4802)
Description	NetApp has released a security update addressing a vulnerability present in GNU C library that is incorporated in their products. **CVE-2025-4802**: GNU C Library versions 2.27 through 2.38 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	Brocade Fabric Operating System Firmware
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250627-0010

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 systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 openSUSE Leap 15.6 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP6 SUSE Real Time Module 15-SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20254139-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254140-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20254141-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40300, CVE-2025-38352, CVE-2025-37838, CVE-2025-21727, CVE-2024-56664, CVE-2024-50061, CVE-2024-35867, CVE-2023-52854)
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Linux versions 20.04 LTS and 18.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7874-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38729, CVE-2025-38718, CVE-2025-39697, CVE-2025-39702, CVE-2025-39757, CVE-2025-40300, CVE-2025-39817, CVE-2025-39849, CVE-2023-53494)
Description	Red Hat 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. Red Hat advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:21760

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.