Advisory Alert

Alert Number: **AAA20250217** **Date:** **February 17, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
NetApp	**High, Medium, Low**	Multiple Vulnerabilities
HPE	Low	Information Disclosure Vulnerability

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40674, CVE-2024-45337)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-40674 -** Multiple NetApp products incorporate libexpat. libexpat versions prior to 2.4.9 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). **CVE-2024-45337 -** Multiple NetApp products incorporate golang.org/x/crypto. golang.org/x/crypto versions prior to 0.31.0 are susceptible to a vulnerability which when successfully exploited could lead to isclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere ONTAP Select Deploy administration utility ONTAP 9 OnCommand Workflow Automation NetApp HCI Compute Node (Bootstrap OS) NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S Data Infrastructure Insights Telegraf Agent (formerly Cloud Insights Telegraf Agent)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20221028-0008/ https://security.netapp.com/advisory/ntap-20250131-0007/

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities
Description	SUSE has released security updates addressing Multiple Linux Kernel Vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Out-of-bound read, Use-after-free, Races condition, Memory leak, NULL pointer diffrence. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5, 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250555-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250556-1 • https://www.suse.com/support/update/announcement/2025/suse-su-20250557-1

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-43680, CVE-2023-27534, CVE-2023-5870, CVE-2023-5869, CVE-2023-5868, CVE-2024-0565, CVE-2023-52426, CVE-2024-28757, CVE-2024-1635, CVE-2023-6536, CVE-2023-6535, CVE-2023-6356, CVE-2023-38709, CVE-2024-24795, CVE-2024-27316, CVE-2024-28752, CVE-2024-24806, CVE-2023-52425, CVE-2024-4741, CVE-2024-4603, CVE-2024-6409, CVE-2024-5535, CVE-2024-4032, CVE-2023-52340, CVE-2024-8096, CVE-2024-21235, CVE-2024-21217, CVE-2024-21210, CVE-2024-21208, CVE-2024-45490, CVE-2024-36886, CVE-2023-4237, CVE-2024-9143, CVE-2024-26882, CVE-2023-52434, CVE-2025-0509, CVE-2021-36084, CVE-2021-36085, CVE-2021-36086, CVE-2021-36087, CVE-2023-6780, CVE-2024-36933)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Security Restrictions Bypass, Information Disclosure, Remote Command Injection. NetApp 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://security.netapp.com/advisory/

Affected Product	**HPE**
Severity	**Low**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2024-39286)
Description	HPE has released security updates addressing an Information Disclosure Vulnerability that exists in their products. **CVE-2024-39286 -** Incorrect execution-assigned permissions in the Linux kernel mode driver for the Intel(R) 800 Series Ethernet Driver before version 1.15.4 may allow an authenticated user to potentially enable information disclosure via local access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Intel E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 Adapter for HPE - Prior to v4.6 • Intel E810-CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter for HPE - Prior to v4.6 • Intel E810-CQDA2 Ethernet 100Gb 2-port QSFP28 OCP3 Adapter for HPE - Prior to v4.6 • Intel E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 Adapter for HPE - Prior to v4.6 • Intel E810-XXVDA2 Ethernet 10/25Gb 2-port SFP28 OCP3 Adapter for HPE - Prior to v4.6 • Intel E810-2CQDA2 Ethernet 100Gb 2-port QSFP28 Adapter for HPE - Prior to v4.6 • Intel E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 MCLK Adapter for HPE - Prior to v4.6 • Intel E810-XXVDA4 Ethernet 10/25Gb 4-port SFP28 OCP3 Adapter for HPE - Prior to v4.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04808en_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.