Advisory Alert

Alert Number: **AAA20250425** **Date:** **April 25, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**High**	OpenSSH Vulnerability
HPE	**Medium**	Privilege Escalation Vulnerability
Ubuntu	**Medium**, **Low**	Linux kernel vulnerabilities

Description

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	OpenSSH Vulnerability (CVE-2024-6387)
Description	NetApp has released security updates addressing an OpenSSH Vulnerability that exists in their products. **CVE-2024-6387 -** Multiple NetApp products incorporate OpenSSH. OpenSSH versions 8.5p1 prior to 9.8p1 are susceptible to a vulnerability referred to as regreSSHion 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 security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 ONTAP tools for VMware vSphere 10, 9 AFF Baseboard Management Controller (BMC) - A1K/A70/A90/A700s Active IQ Unified Manager for VMware vSphere E-Series SANtricity OS Controller Software 11.x FAS/AFF Baseboard Management Controller (BMC) - 8300/8700/A400/C400 FAS/AFF Baseboard Management Controller (BMC) - A250/500f/C250 FAS/AFF Baseboard Management Controller (BMC) - A800/C800/A900/9500 FAS/AFF Baseboard Management Controller (BMC) - C190/A150/A220/FAS2720/FAS2750 FAS/AFF Baseboard Management Controller (BMC) - FAS2820 ONTAP Select Deploy administration utility
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240701-0001/

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-37088)
Description	HPE has released security updates addressing a Privilege Escalation Vulnerability that exists in their products. **CVE-2025-37088 -** A security vulnerability has been identified in HPE Cray Data Virtualization Service (DVS). Depending on the race conditions and configuration, this vulnerability may lead to local/cluster unauthorized access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Cray Supercomputing Operating System Software prior to COS 23.11.4 (COS Base 3.0.4/USS 1.0.4) COS 25.1 (COS Base 3.2.0/USS 1.2.0) COS 24.10.1 (COS Base 3.1.2/USS 1.1.2-2)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04749en_us&docLocale=en_US

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Linux kernel vulnerabilities (CVE-2025-21703, CVE-2024-56651, CVE-2024-50248, CVE-2025-21701, CVE-2024-26837, CVE-2024-46826, CVE-2025-21993, CVE-2025-21702, CVE-2024-50256, CVE-2025-21756, CVE-2025-21700, CVE-2024-53237, CVE-2021-47119, CVE-2024-35958, CVE-2024-49974, CVE-2024-26915)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause denial of service, system crash, out-of-bounds write, privileges escalate. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7455-1 • https://ubuntu.com/security/notices/USN-7461-1

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.