FINCSIRT

Advisory Alert

Alert Number: **AAA20241111** **Date:** **November 11, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
NetApp	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Unauthorized Access, Denial of Service and Buffer Overflow. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Cray XD665 - Prior to 1.50 (Cray SC XD665 Firmware Pack 2024.09.00) HPE Cray XD670 - Prior to 2.01 HPE Cray EX235a Accelerator Blade - Prior to 1.9.0 (HFP 24.9.0) HPE Cray EX235n Server - Prior to 1.4.0 (HFP 24.8.1) HPE Cray EX254n Accelerator Blade - Prior to 1.9.0 (HFP 24.8.1) HPE Cray EX255a Accelerator Blade - Prior to 1.1.1 (HFP 24.9.0) HPE Cray EX420 Compute Blade - Prior to 1.3.2 (HFP 24.8.1) HPE Cray EX425 Compute Blade - Prior to 1.7.4 (HFP 24.8.1) HPE Cray EX4252 Compute Blade - Prior to 1.7.0 (HFP 24.9.0) HPE ProLiant XL645d Gen10 Plus Server - Prior to v3.10 (HFP 24.8.1) HPE ProLiant XL675d Gen10 Plus Server - Prior to v3.10 (HFP 24.8.1)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04732en_us&docLocale=en_US

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26641, CVE-2024-21994)
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 system. **CVE-2024-26641 -** Certain versions of Linux kernel are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or Denial of Service (DoS) **CVE-2024-21994 -** StorageGRID (formerly StorageGRID Webscale) versions prior to 11.9.0 are susceptible to a Denial of Service (DoS) vulnerability. Successful exploit by an authenticated attacker could lead to a service crash. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FAS/AFF Baseboard Management Controller (BMC) - C190/A150/A220/FAS2720/FAS2750 StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20241108-0001/ • https://security.netapp.com/advisory/ntap-20241108-0008/

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.