Advisory Alert

| Alert Number: | AAA20231127 | Date: | November 27, 2023 |

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-38087, CVE-2023-32252, CVE-2023-3489)
Description	NetApp has released security updates addressing multiple Vulnerabilities in their products. **CVE-2022-38087** - Certain versions of Intel BIOS Firmware are susceptible to a vulnerability which when successfully exploited could allow escalation of privilege and information disclosure via local access **CVE-2023-32252** - Linux kernel versions prior to 6.4-rc1 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2023-3489** - Several commands in Brocade Fabric OS v9.2.0 could log the FTP/SFTP/SCP server password in clear text in the SupportSave file when performing a downgrade from Fabric OS v9.2.0 to any earlier version of Fabric OS. NetApp recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	NetApp HCI Compute Node BIOS NetApp HCI Storage Node BIOS NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S NetApp HCI Baseboard Management Controller (BMC) - H410C Brocade Fabric Operating System Firmware
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20231124-0006/ https://security.netapp.com/advisory/ntap-20231124-0001/ https://security.netapp.com/advisory/ntap-20231124-0003/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaPay Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public   Report incidents to incident@fincsirt.lk   TLP: WHITE