TLP: WHITE

Advisory Alert

Alert Number: **AAA20251224** **Date:** **December 24, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Out-of-bounds Read Vulnerability
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Out-of-bounds Read Vulnerability (CVE-2025-5318)
Description	IBM has released security updates addressing an Out-of-bounds Read Vulnerability that exists in the libssh library which affects IBM Total Storage Service Console. **CVE-2025-5318** - A flaw was found in the libssh library in versions less than 0.11.2. An out-of-bounds read can be triggered in the sftp_handle function due to an incorrect comparison check that permits the function to access memory beyond the valid handle list and to return an invalid pointer, which is used in further processing. This vulnerability allows an authenticated remote attacker to potentially read unintended memory regions, exposing sensitive information or affect service behavior. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Total Storage Service Console (TSSC) / TS4500 IMC versions: 9.4.14, 9.4.21, 9.4.26, 9.4.31, 9.5.8, 9.6.10, 9.6.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7255352

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1292, CVE-2022-1343, CVE-2022-1434, CVE-2022-1473, CVE-2022-2068, CVE-2022-0778, CVE-2021-4160)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause disclosure of sensitive information, addition or modification of data and Denial of Service. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere AFF Baseboard Management Controller (BMC) - A700s Brocade Fabric Operating System Firmware Brocade SAN Navigator (SANnav) Cloud Volumes ONTAP Mediator E-Series SANtricity OS Controller Software 11.x FAS/AFF Baseboard Management Controller (BMC) - 9500/8700/8300 FAS/AFF Baseboard Management Controller (BMC) - A900/A800/A400/A250/A220/A150 FAS/AFF Baseboard Management Controller (BMC) - 500f FAS/AFF Baseboard Management Controller (BMC) - C800/C400/C250/C190 FAS/AFF Baseboard Management Controller (BMC) - FAS2720/FAS2750 NetApp SolidFire & HCI Storage Node (Element Software) ONTAP Antivirus Connector ONTAP Select Deploy administration utility
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20220602-0009 • https://security.netapp.com/advisory/ntap-20220707-0008 • https://security.netapp.com/advisory/ntap-20220321-0002 • https://security.netapp.com/advisory/ntap-20220204-0005

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.