Advisory Alert

Alert Number: AAA20250606 **Date:** June 6, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
NetApp	**High**	Multiple Vulnerabilities
Hitachi	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Samba	**Medium**	Authorization Cache Staleness Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2025-30065)
Description	IBM has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in Apache Parquet which affects IBM Db2. **CVE-2025-30065** - Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code Users are recommended to upgrade to version 1.15.1, which fixes the issue. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7235042

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-32415, CVE-2024-29133, CVE-2025-32414)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-32415/CVE-2025-32414** - Multiple NetApp products incorporate libxml2. Libxml2 versions prior to 2.13.8 and 2.14.0 prior to 2.14.2 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2024-29133** - Multiple NetApp products incorporate Apache Commons Configuration. Apache Commons Configuration versions 2.0 prior to 2.10.1 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). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S NetApp HCI Baseboard Management Controller (BMC) - H410C NetApp HCI Compute Node (Bootstrap OS) ONTAP tools for VMware vSphere 10 SnapCenter
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250605-0003 • https://security.netapp.com/advisory/ntap-20250605-0002 • https://security.netapp.com/advisory/ntap-20250605-0004

Affected Product	**Hitachi**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in Microsoft products which affect Hitachi Disk Array Systems. These vulnerabilities could be exploited by malicious users to compromise the affected system. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H, 5100, 5500, 5100H, 5500H Hitachi Virtual Storage Platform G1000, G1500, F1500 Hitachi Virtual Storage Platform VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2025/04.html

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3510, CVE-2022-3509, CVE-2022-3171, CVE-2025-3050, CVE-2024-23454, CVE-2024-49350, CVE-2024-52903, CVE-2025-0915, CVE-2025-1000, CVE-2025-1493, CVE-2025-1992, CVE-2024-7254)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2. These vulnerabilities could be exploited by malicious users to cause Denial of Service and Sensitive Information Disclosure. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7234906 • https://www.ibm.com/support/pages/node/7235067 • https://www.ibm.com/support/pages/node/7235073 • https://www.ibm.com/support/pages/node/7235070 • https://www.ibm.com/support/pages/node/7235069 • https://www.ibm.com/support/pages/node/7232336 • https://www.ibm.com/support/pages/node/7232529 • https://www.ibm.com/support/pages/node/7232528 • https://www.ibm.com/support/pages/node/7232518 • https://www.ibm.com/support/pages/node/7232515

Affected Product	**Samba**
Severity	**Medium**
Affected Vulnerability	Authorization Cache Staleness Vulnerability (CVE-2025-0620)
Description	Samba has released security updates addressing an Authorization Cache Staleness Vulnerability that exists in their products. **CVE-2025-0620** - With Kerberos authentication SMB sessions typically have an associated lifetime, requiring re-authentication by the client when the session expires. As part of the re-authentication, Samba receives the current group membership information and is expected to reflect this change in further SMB request processing. Samba advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Samba 4.22.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/history/samba-4.22.2.html

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.