Advisory Alert

Alert Number: AAA20250124 **Date:** January 24, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**Critical**	Pre-Authentication Remote Command Execution Vulnerability
QNAP	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple sensitive information disclosure vulnerabilities

Description

Affected Product	**SonicWALL**
Severity	**Critical**
Affected Vulnerability	Pre-Authentication Remote Command Execution Vulnerability (CVE-2025-23006)
Description	SonicWALL has released security updates to address a Pre-Authentication Remote Command Execution Vulnerability in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which, under specific conditions, could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands SonicWALL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 (platform-hotfix) and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002

Affected Product	**QNAP**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-12084 ,CVE-2024-12085 ,CVE-2024-12086 ,CVE-2024-12087 ,CVE-2024-12088 ,CVE-2024-12747)
Description	QNAP has released security updates addressing Multiple Vulnerabilities affecting HBS 3 Hybrid Backup Sync. These vulnerabilities could be exploited by malicious users to compromise the affected system. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HBS 3 Hybrid Backup Sync 25.1.x versions before 25.1.4.952
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-25-02

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple sensitive information disclosure vulnerabilities (CVE-2023-38729, CVE-2021-29825)
Description	IBM has released security updates to address multiple sensitive information disclosure vulnerabilities in their products. **CVE-2023-38729 -** IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server)10.5, 11.1, and 11.5 is vulnerable to sensitive information disclosure when using ADMIN_CMD with IMPORT or EXPORT **CVE-2021-29825 -** IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information when using ADMIN_CMD with LOAD or BACKUP IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 10.5.0.x IBM Db2 11.1.4.x IBM Db2 11.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145721 • https://www.ibm.com/support/pages/node/6489499

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.