TLP: WHITE

Advisory Alert

Alert Number: **AAA20240109** **Date:** **January 9, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
NETGEAR	**Medium**	Post-Authentication Stack Overflow Vulnerability

Description

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-47158, CVE-2023-47141, CVE-2023-47145, CVE-2023-45193, CVE-2023-47747, CVE-2023-27859, CVE-2023-47746, CVE-2023-50308, CVE-2023-47152)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2 . If exploited, these vulnerabilities could lead to sensitive information disclosure, denial of service, privilege escalation, and remote code execution. It is recommended by IBM to apply the necessary security fixes at earliest to avoid issues.
Affected Products	IBM Db2 10.5.0.xServer IBM Db2 11.1.4.xServer IBM Db2 11.5.x Server IBM Db2 11.5.9 Client IBM Db2 10.5.0.xClient (RTCL) IBM Db2 11.1.4.xClient (RTCL) IBM Db2 11.5.x Client (RTCL) IBM Db2 11.5.x Client
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7105496 https://www.ibm.com/support/pages/node/7105497 https://www.ibm.com/support/pages/node/7105499 https://www.ibm.com/support/pages/node/7105500 https://www.ibm.com/support/pages/node/7105501 https://www.ibm.com/support/pages/node/7105502 https://www.ibm.com/support/pages/node/7105503 https://www.ibm.com/support/pages/node/7105505 https://www.ibm.com/support/pages/node/7105506 https://www.ibm.com/support/pages/node/7105605

Affected Product	**NETGEAR**
Severity	**Medium**
Affected Vulnerability	Post-Authentication Stack Overflow Vulnerability
Description	NETGEAR has released a security update addressing post-authentication stack overflow security vulnerability in multiple NETGEAR Routers and WiFi Systems. It is recommended by NETGEAR to apply the necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Routers and WiFi Systems
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.netgear.com/000065939/Security-Advisory-for-Post-Authentication-Stack-Overflow-on-Some-Routers-and-WiFi-Systems-PSV-2019-0222

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.