TLP: WHITE

Advisory Alert

Alert Number: **AAA20241108** **Date:** **November 8, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetGear	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**NetGear**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	NetGear has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Sensitive Information Disclosure, Cross Site Scripting, Security Misconfiguration. NetGear advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Insight prior to firmware version 7.4 RBK852 prior to firmware version 7.2.6.21 RBR850 prior to firmware version 7.2.6.21 RBS850 prior to firmware version 7.2.6.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://kb.netgear.com/000066414/Security-Advisory-for-Security-Misconfiguration-on-Some-WiFi-Systems-PSV-2021-0183 • https://kb.netgear.com/000066412/Security-Advisory-for-Sensitive-Information-Disclosure-on-Insight-PSV-2024-0053 • https://kb.netgear.com/000066413/Security-Advisory-for-Reflected-Cross-Site-Scripting-on-Insight-PSV-2024-0035

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40094, CVE-2024-45654, CVE-2024-47764, CVE-2024-43800, CVE-2024-43796, CVE-2024-43799, CVE-2024-45296, CVE-2024-39338, CVE-2024-45590)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Perform Unauthorized Actions, Cross-site Scripting, Server-side Request Forgery. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty - Versions 20.0.0.6 - 24.0.0.11 IBM Security QRadar EDR - Versions 3.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7174997 • https://www.ibm.com/support/pages/node/7175072 • https://www.ibm.com/support/pages/node/7175086

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.