Advisory Alert

Alert Number: **AAA20231218** **Date:** **December 18, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Watchguard	**High**	FRR Dynamic Routing Denial of Service Vulnerabilities
IBM	**Medium**	Sensitive information disclosure vulnerability

Description

Affected Product	**Watchguard**
Severity	**High**
Affected Vulnerability	FRR Dynamic Routing Denial of Service Vulnerabilities (CVE-2023-38802, CVE-2023-41358)
Description	Watchguard has released security updates addressing FRR Dynamic Routing Denial of Service Vulnerabilities BGP software such as FRRouting FRR and Quagga included as part of Fireware OS enable a remote attacker to incorrectly reset network sessions through an invalid BGP update. This vulnerability is only applicable to Firebox appliances with BGP routing features enabled. Watchguard recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Watchguard Firebox - Fireware OS 12.2.1 up to and including 12.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2023-00010

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Sensitive information disclosure vulnerability (CVE-2023-47741)
Description	IBM has released security updates addressing a Sensitive information disclosure vulnerability within their products. **CVE-2023-47741** - IBM Db2 Mirror for i GUI web browser client interface implementation could allow sensitive information, including passwords, to be left in memory, which could be viewed using common tools for viewing process information on a PC. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 Mirror for i 7.4 IBM Db2 Mirror for i 7.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7097801

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.