Advisory Alert

Alert Number: AAA20230915 **Date:** September 15, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**High**	Access bypass vulnerability
IBM DB2	**High**	Information disclosure vulnerability
IBM QRadar SIEM	**Medium**	Denial of service

Description

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Access bypass vulnerability
Description	Drupal has released security updates addressing Access bypass vulnerability that exist in the Mail login module. Drupal core contains protection against brute force attacks via a flood control mechanism. This module's functionality did not replicate the flood control, enabling brute force attacks. This module enables users to log in by email address with minimal configurations Drupal recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Mail_login module less than 2.8.0 for Drupal 8 or 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2023-045

Affected Product	**IBM DB2**
Severity	**High**
Affected Vulnerability	Information disclosure vulnerability (CVE-2023-30441)
Description	IBM has released security updates addressing Information disclosure vulnerability that exist in the DB2 Recovery Expert. IBM Runtime Environment, Java Technology Edition IBMJCEPlus and JSSE 8.0.7.0 through 8.0.7.11 components could expose sensitive information using a combination of flaws and configurations. IBM recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	DB2 Recovery Expert for LUW 5.5.0.1 DB2 Recovery Expert for LUW 5.5.0.1 IF1 DB2 Recovery Expert for LUW 5.5.0.1 IF2 DB2 Recovery Expert for LUW 5.5.0.1 IF3 DB2 Recovery Expert for LUW 5.5.0.1 IF4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7031999

Affected Product	**IBM QRadar SIEM**
Severity	**Medium**
Affected Vulnerability	Denial of service (CVE-2022-25883,CVE-2023-26115)
Description	IBM has released security updates addressing Denial of service that exist in the IBM QRadar. **CVE-2022-25883** - Versions of the package semver before 7.5.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the function new Range, when untrusted user data is provided as a range. **CVE-2023-26115** - All versions of the package word-wrap are vulnerable to Regular Expression Denial of Service (ReDoS) due to the usage of an insecure regular expression within the result variable. IBM recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM QRadar Pulse App 1.0.0 - 2.2.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7032220

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.