Advisory Alert

Alert Number: AAA20201119 **Date:** November 19, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM DB2	**High**	Arbitrary code execute
Drupal	**High**	Remote code execution

Description

Affected Product	**IBM DB2**
Severity	**High**
Affected Vulnerability	Arbitrary code execute (CVE-2020-4701)
Description	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) could cause a buffer overflow due to improper bounds checking. It could allow a local attacker to execute arbitrary codes on the system as an authenticated root user.
Affected Products	IBM Db2 V10.5, V11.1, V11.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6370025

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Remote code execution (CVE-2020-13671)
Description	Drupal core does not properly sanitize certain file names on uploaded files, which can lead to files being interpreted as the incorrect extension and served as the wrong file extension type or executed as PHP for certain hosting configurations. Additionally, it's recommended that you audit all previously uploaded files to check for malicious extensions. In which as a solution, update to Drupal's latest versions. Drupal 8 prior to 8.8.x are end-of-life and does not receive security updates.
Affected Products	Drupal 9.0 Drupal 8.9 Drupal 8.8 or earlier Drupal 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2020-012

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.