Advisory Alert

Alert Number: AAA20211119 **Date:** November 19, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	Critical	Multiple Vulnerabilities

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Cross Site Scripting
Description	Drupal has released security patch updates addressing Cross Site Scripting that exists in Drupal core. Drupal is vulnerable when it is configured to allow use of the CKEditor library for WYSIWYG editing. An attacker with capability to create or edit content (even without access to CKEditor themselves) may be able to exploit one or more Cross-Site Scripting (XSS) vulnerabilities to target users with access to the WYSIWYG CKEditor, including the site admins who has privileged access.
Affected Products	If you are using Drupal 9.2, update to Drupal 9.2.9. If you are using Drupal 9.1, update to Drupal 9.1.14. If you are using Drupal 8.9, update to Drupal 8.9.20.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2021-011

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.