



Advisory Alert

Alert Number: AAA20210813

Date: August 13, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	Critical	Cross Site Scripting

Description

Affected Product	Drupal
Severity	Critical
Affected Vulnerability	Cross Site Scripting
Description	Multiple Cross Site Scripting vulnerabilities are possible if drupal is configured to allow use of the CKEditor library for WYSIWYG editing. An attacker that can create or edit content (even without access to CKEditor themselves) may be able to exploit one or more Cross Site Scripting vulnerabilities to target users with access to the WYSIWYG CKEditor, including site admins with privileged access.
Affected Products	If you are using Drupal 9.2, update to Drupal 9.2.4. If you are using Drupal 9.1, update to Drupal 9.1.12. If you are using Drupal 8.9, update to Drupal 8.9.18.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2021-005

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.