



Advisory Alert

Alert Number: AAA20220318 Date: March 18, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Durpal	Critical	Cross-Site Scripting Vulnerability

Description

Affected Product	Durpal
Severity	Critical
Affected Vulnerability	Cross site scripting vulnerability (CVE-2022-24728, CVE-2022-24729)
Description	Durpal has issued Security Updates to address a cross site scripting vulnerability that exists in their product. Drupal becomes vulnerable if configured to allow the usage 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 (XSS) vulnerabilities to target users with access to the WYSIWYG CKEditor, including site admins with privileged access.
Affected Products	Drupal 9.3 Drupal 9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-005

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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777