TLP: WHITE

Advisory Alert

Alert Number : **AAA20200917** **Date :** **September 17, 2020**

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**High**	Multiple Vulnerabilities

Description

Affected Product	Drupal
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-13670) , (CVE-2020-13667) , (CVE-2020-13668) (CVE-2020-13666) , (CVE-2020-13669)
Description	The Drupal Content Manager has released 5 security updates to mitigate recently discovered vulnerabilities in its kernel. **CVE-2020-13670** : Drupal indicate that there is an information disclosure vulnerability in the file module that would allow an attacker to gain access to the metadata of a private permanent file to which the attacker does not have access by guessing the ID of the file. **CVE-2020-13667**: Drupal indicate that the experimental workspaces module does not sufficiently verify access permissions when changing workspaces, which generates an access bypass vulnerability. An attacker could see the content before the site owner publish the drafts to the live workspace. **CVE-2020-13668**: Drupal 8 and 9 have a reflected cross-site scripting (XSS) vulnerability in HTML forms that occurs under certain circumstances. **CVE-2020-13666**: Drupal AJAX API does not disable JSONP by default, which can lead to cross-site scripting. **CVE-2020-13669**: Drupal they indicate that the CKEditor image captioning functionality built into Drupal is vulnerable to cross-site scripting (XSS).
Affected Products	Drupal 7.x Drupal 8.8.x Drupal 8.9.x Drupal 9.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2020-011 https://www.drupal.org/sa-core-2020-008 https://www.drupal.org/sa-core-2020-009 https://www.drupal.org/sa-core-2020-007 https://www.drupal.org/sa-core-2020-010

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.