Advisory Alert

Alert Number: AAA20210928 **Date:** September 28, 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	Multiple Vulnerabilities
Description	Drupal has released security updates addressing multiple vulnerabilities that exists in their products including Arbitrary PHP code execution, Access bypass, Information Disclosure, Cross-site scripting, Cache poisoning, Cross-Site Request Forgery, SAML miss-configurations. An attacker could exploit these vulnerabilities by sending the specially crafted requests.
Affected Products	Taxonomy Manager module for Drupal 8 or 9 SAML Service Provider module for Drupal 8.x or 9.x or 7.x domain_group module for Drupal 8.x,9.x TB Mega Menu module for Drupal 8.x user_hash module for Drupal 8 or 9 cshs module for Drupal 8 or 9 Commerce module for Drupal 8.x File Extractor 2.0.2 or below,File Extractor 3.0.0, 4.0.0 search_api_attachments module for Drupal 7.x-1.19
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2021-034 https://www.drupal.org/sa-contrib-2021-033 https://www.drupal.org/sa-contrib-2021-032 https://www.drupal.org/sa-contrib-2021-031 https://www.drupal.org/sa-contrib-2021-030 https://www.drupal.org/sa-contrib-2021-041 https://www.drupal.org/sa-contrib-2021-040 https://www.drupal.org/sa-contrib-2021-039 https://www.drupal.org/sa-contrib-2021-038 https://www.drupal.org/sa-contrib-2021-037 https://www.drupal.org/sa-contrib-2021-036 https://www.drupal.org/sa-contrib-2021-035

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.