Advisory Alert

Alert Number: AAA20220613 **Date:** June 13, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Medium**	Information Disclosure

Description

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Information Disclosure (CVE-2022-31042, CVE-2022-31043)
Description	Durpal has released a workaround/patch for flows that exists in Guzzle library. The Guzzle library is used for handling HTTP requests and responses to external services. Both of these flows were occurred as result of failure to strip the cookie header on change in host or HTTP and fix failure to strip authorization header on. These flaws are not affecting to the drupal core, but may affect some contributed projects or custom code on Drupal sites. Drupal has recommended to apply the available patch updates.
Affected Products	Drupal 9.4 Drupal 9.3 Drupal 9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-011

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.