



Advisory Alert

Alert Number : AAA20201127

Date : November 27, 2020

Document Classification Level : **Public Circulation Permitted**Information Classification Level : **TLP: WHITE**

Overview

Product	Severity	Vulnerability
Durpal	Critical	Arbitrary PHP code execution

Description

Affected Product	Durpal
Severity	Critical
Affected Vulnerability	Arbitrary PHP code execution (CVE-2020-28949, CVE-2020-28948)
Description	PEAR Archive_Tar library product has released security patch updates addressing multiple vulnerabilities that impacts Durpal which has arbitrary PHP code execution vulnerability. Multiple vulnerabilities are possible if Drupal is configured to allow .tar, .tar.gz, bz2, or .tlz file uploads and processes them. To mitigate this issue its required to prevent untrusted users from uploading .tarm, .tar.gz, bz2, .tlz files to the system.
Affected Products	Drupal 9.0 , Drupal 8.8 , Drupal 8.9 , Drupal 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2020-013

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.