Advisory Alert

Alert Number: AAA20210429 **Date:** April 29, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Access bypass
Cisco	**High**	Multiple vulnerabilities

Description

Affected Product	Drupal
Severity	**Critical**
Affected Vulnerability	Access bypass
Description	The SAML Authentication module allows users to authenticate against a SAML identity provider to login to your Drupal site. The module doesn't sufficiently protect against unauthorized local access, by way of using the password reset facility, for users who are supposed to only be able to log in through the identity provider. This creates a scenario where after such a user is blocked from logging in through the identity provider but not explicitly blocked in Drupal, they are still able to log in by sending themselves a Drupal 'password reset' e-mail.
Affected Products	All versions of Drupal 8/9, upgrade to samlauth 8.x-3.1 Drupal 7, upgrade to samlauth 7.x-1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2021-006

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-1493, CVE-2021-1495, CVE-2021-1402, CVE-2021-1256, CVE-2021-1448, CVE-2021-1455 CVE-2021-1456, CVE-2021-1457, CVE-2021-1458, CVE-2021-1477, CVE-2021-1369, CVE-2021-1489, CVE-2021-1445, CVE-2021-1504, CVE-2021-1501, CVE-2021-1476, CVE-2021-1488, CVE-2020-3580, CVE-2020-3581, CVE-2020-3582, CVE-2020-3583)
Description	Cisco has released updates addressing multiple vulnerabilities that exists in Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software. It is highly recommended to apply necessary fixes provided in official Cisco website at earliest to avoid these vulnerabilities.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&last_published=2021%20Apr&sort=-day_sir#~Vulnerabilities

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.