Advisory Alert

Alert Number: AAA20220929 **Date:** September 29, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**High**	Directory Traversal Vulnerability
Cisco	**High, Medium**	Multiple Vulnerabilities
Drupal	**Medium**	Access bypass Vulnerability

Description

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Directory Traversal Vulnerability (CVE-2022-39261)
Description	Durpal has released Security Updates addressing a high severity vulnerability that exist In the third party library named as Twig that is used for content templating and sanitization. Using this vulnerability that exists in the Twig, its possible use the source or include statement to read arbitrary files from outside the templates directory when using a namespace like @somewhere/../some.file When using the file system loader to load templates for which the name is a user input. Because of this Multiple vulnerabilities are possible if an untrusted user has access to write Twig code, including potential unauthorized read access to private files, the contents of other files on the server, or database credentials. Drupal highly recommends to apply necessary fixes at earliest to avoid issues.
Affected Products	Drupal 9.4 Drupal 9.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2022-016

Affected Product	**Cisco**
Severity	**High , Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20848, CVE-2022-20769, CVE-2022-20847, CVE-2022-20920, CVE-2022-20662, CVE-2022-20775,CVE-2022-20810,CVE-2022-20818,CVE-2022-20830,CVE-2022-20837,CVE-2022-20844, , CVE-2022-20851,CVE-2022-20855,CVE-2022-20856,CVE-2022-20864,CVE-2022-20870,CVE-2022-20915,CVE-2022-20919, CVE-2022-20930, CVE-2022-20944,CVE-2022-20945)
Description	Cisco has released security updates addressing multiple vulnerabilities which may lead attackers to cause Denial of Service, Privilege Escalation, Arbitrary Code Execution, Command Injection, Arbitrary File Corruption, Authentication Bypass, and Information Disclosure. Cisco highly recommends to apply necessary fixes at earliest to avoid issues.
Affected Products	• Cisco Embedded Wireless Controller on Catalyst 9100 Access Points • Cisco WLC AireOS Software • Catalyst 9800-CL Wireless Controllers for Cloud • Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300, 9400, and 9500 Series Switches • Catalyst 9800 Series Wireless Controllers • Embedded Wireless Controllers on Catalyst Access Points • Cisco IOS or IOS XE Software • Cisco SD-WAN Software • Cisco Catalyst 3650, • Catalyst 3850 • Catalyst 9000 Family Switches • Cisco Catalyst 9200 Series Switches • Catalyst Access Points • Catalyst 9800-CL Wireless Controllers for Cloud • Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches • Catalyst 9800 Series Wireless Controllers • Cisco Catalyst 9100 Series APs • SD-WAN vBond Orchestrator Software • SD-WAN vEdge Routers • SD-WAN vManage Software • SD-WAN vSmart Controller Software • Cisco vManage that have SD-AVC enabled. • Catalyst 3600 Series Switches • Catalyst 3800 Series Switches • Catalyst 9200 Series Switches • Catalyst 9300 Series Switches • Catalyst 9400 Series Switches • Catalyst 9500 Series Switches • Catalyst 9600 Series Switches • Catalyst 9800-CL Wireless Controllers for Cloud • Catalyst 9800 Embedded Wireless Controller for Catalyst 9300, 9400, and 9500 Series Switches • Catalyst 9800 Series Wireless Controllers • Embedded Wireless Controller on Catalyst Access Points • Cisco IOS XE SD-WAN Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&keyword=2022%20Sep%2028&sort=-day_sir#~Vulnerabilities

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access bypass vulnerability
Description	Durpal has released Security Updates addressing Access bypass vulnerability. This vulnerability is mitigated by the fact that an attacker must obtain a method to access arbitrary file paths, the site must have public or private takeover enabled, and the file metadata cache must be ignored.. Drupal recommended applying necessary updates at the earliest to avoid issues.
Affected Products	S3 File System module for Drupal 7.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2022-057

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.