Hive Pro

THREAT ADVISORY

Major Content Management Systems affected by Multiple vulnerabilities

TA2022067

Threat Level AMBER

Publish Date – March 18, 2022

Several flaws in well-known content management systems WordPress and Drupal have been uncovered. A content management system, or CMS, is software that allows users to create, manage, and edit website content without requiring specialist technical skills. WordPress Core and Drupal's CKEditor library both are impacted by these vulnerabilities.

The three vulnerabilities affecting WordPress Core versions prior to 5.9.2 could allow attackers to run arbitrary JavaScript in a user's session by enticing a victim user into clicking a link. An attacker who successfully exploited these flaws may insert malicious JavaScript into a post, which would then execute when viewed by an administrator. Several methods, including the addition of new malicious administrative users and the injection of backdoors into a website, can be used to take over a site using JavaScript running in an administrator's session.

CKEditor is an open-source HTML editor library which if configured with Drupal allows an attacker to generate or edit content by exploiting one or more Cross-Site Scripting (XSS) vulnerabilities.

The WordPress vulnerabilities have been fixed in the version 5.9.2 and the Drupal CKEditor vulnerabilities has been fixed in the versions 9.3.8 and 9.2.15. Organizations can patch these vulnerabilities using the patch links given below.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
TA0001: Initial Access
TA0009: Collection
TA0006: Credential Access
TA0002: Execution
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
T1557: Adversary-in-the-Middle
T1190: Exploit Public-Facing Application
T1059: Command and Scripting Interpreter
T1059.007: Command and Scripting Interpreter: JavaScript/JScript
T1204.001: User Execution: Malicious Link

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
Unassigned	WordPress Core versions 5.9.0-5.9.1	cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*	Contributor+ Stored XSS	CWE-79
Unassigned	WordPress Core version 5.9.2 and earlier		Prototype Pollution via the Gutenberg wordpress/url package	CWE-1321
CVE-2021-20083	WordPress Core version 5.9.2 and earlier		Prototype Pollution in jQuery	CWE-1321
CVE-2022-24728	CKEditor 4 version 4.18.0 and earlier	cpe:2.3:a:ckeditor:ckeditor:*:*:*:*:*:*:*:*	HTML processing vulnerability allowing to execute JavaScript code	CWE-79
CVE-2022-24729	CKEditor 4 version 4.18.0 and earlier		Regular expression Denial of Service in dialog plugin	CWE-400

Patch Link

https://www.drupal.org/project/drupal/releases/9.2.15
https://www.drupal.org/project/drupal/releases/9.3.8
https://wordpress.org/news/2022/03/wordpress-5-9-2-security-maintenance-release/

References

https://www.wordfence.com/blog/2022/03/wordpress-5-9-2-security-update-fixes-xss-and-prototype-pollution-vulnerabilities/
https://www.drupal.org/sa-core-2022-005