

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



Code Execution and Other Vulnerabilities Patched in Drupal

By [Eduard Kovacs](#) on July 22, 2022

Share

Tweet

推荐 11



Drupal developers have announced the release of updates that patch several vulnerabilities in the open source content management system (CMS).

Drupal has released four [advisories](#) that describe four types of vulnerabilities. One of them has been rated “critical” and the other three “moderately critical.” Drupal uses the NIST Common Misuse Scoring System to rate vulnerabilities — instead of CVSS — with flaws being rated “less critical,” “moderately critical,” “critical” and “highly critical.”

The “critical” vulnerability, tracked as [CVE-2022-25277](#), affects Drupal 9.3 and 9.4. The issue impacts the Drupal core and it can lead to arbitrary PHP code execution on Apache web servers by uploading specially crafted files.

Drupal developers pointed out that only Apache web servers are impacted and only with specific configurations. They have advised website admins to check their server for possible signs of compromise.

The three “moderately critical” security holes also impact the Drupal core. Their exploitation can lead to cross-site scripting (XSS) attacks, information disclosure, or access bypass.

Patches for these vulnerabilities are included in Drupal 9.4.3 and 9.3.19. The information disclosure flaw also impacts Drupal 7 and a fix has been included in version 7.91.

The US Cybersecurity and Infrastructure Security Agency (CISA) has [advised Drupal users](#) to review the advisories and install the updates.

While Drupal websites are not as targeted as WordPress sites, several of the vulnerabilities found in the CMS in the past years were [exploited](#) by malicious actors, including for [spam campaigns](#) and to [hack websites and deliver malware](#).

Related: [Access Bypass, Data Overwrite Vulnerabilities Patched in Drupal](#)

Related: [Drupal Patches 'High-Risk' Third-Party Library Flaws](#)

Related: [Drupal Releases Out-of-Band Security Updates Due to Availability of Exploits](#)

Share

Tweet

推荐 11



Eduard Kovacs ([@EduardKovacs](#)) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

[Chrome Flaw Exploited by Israeli Spyware Firm Also Impacts Edge, Safari](#)

[New Cross-Platform 'Luna' Ransomware Only Offered to Russian Affiliates](#)

[Code Execution and Other Vulnerabilities Patched in Drupal](#)

[Exploitation of Recent Chrome Zero-Day Linked to Israeli Spyware Company](#)

[Hundreds of ICS Vulnerabilities Disclosed in First Half of 2022](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

sponsored links

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

[2022 Singapore/APAC ICS Cyber Security Conference](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

Tags:

[NEWS & INDUSTRY](#) [Vulnerabilities](#)

Search

Get the Daily Briefing

BRIEFING

Business Email Address

Subscribe

