Several Access Bypass, CSRF Vulnerabilities Patched in Drupal

By Eduard Kovacs on September 16, 2021

Drupal developers on Wednesday informed users that updates released for Drupal 8.9, 9.1 and 9.2 patch five vulnerabilities that can be exploited for cross-site request forgery (CSRF) and access bypass.

Three of the flaws are related to access bypass. They involve the JSON:API, REST/File, and QuickEdit modules, and they can allow an attacker to access data or upload arbitrary files, but certain conditions need to be met for an attack to work.

As for the CSRF flaws, they impact the Media and QuickEdit modules. According to Drupal developers, their exploitation could lead to HTML code injection into a page accessed by a trusted user and possible data integrity issues, respectively.

All of the vulnerabilities have been assigned a moderately critical severity rating. It's worth noting that Drupal classifies vulnerabilities based on the NIST Common Misuse Scoring System and moderately critical is roughly the equivalent of medium severity in the Common Vulnerability Scoring System (CVSS).

The vulnerabilities have been patched with the release of versions 9.2.6, 9.1.13 and 8.9.19. Drupal 7 is not affected, and Drupal 8 prior to 8.9.x and Drupal 9 prior to 9.1.x have reached end of life and will not be receiving fixes.

This is the sixth round of security updates released this year for Drupal. Drupal is not targeted by hackers as much as WordPress, which is not surprising considering that Drupal is only used on 1% of sites while WordPress is used by more than 42%. However, hackers targeting Drupal websites in mass attacks is not unheard of so users should not ignore security patches.

Related: Drupal Releases Out-of-Band Security Updates Due to Availability of Exploits

Related: Remote Code Execution Vulnerability Patched in Drupal

Related: Drupal Updates CKEditor to Patch XSS Vulnerabilities

Related: Information Disclosure, XSS Vulnerabilities Patched in Drupal

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:
Several Access Bypass, CSRF Vulnerabilities Patched in Drupal
Links Found Between MSHTML Zero-Day Attacks and Ransomware Operations
Regular Users Can Now Remove Password From Their Microsoft Account
Cloud Backup Company Rewind Raises $65 Million
ICS Patch Tuesday: Siemens, Schneider Electric Address Over 40 Vulnerabilities

Tags:
NEWS & INDUSTRY Vulnerabilities