بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

به‌روزرسانی چندین آسیب‌پذیری در سیستم مدیریت محتوای دروپال

آسیب‌پذیری

شناسه سند ..... Maher_13990629….

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۰۶/۲۹

طبقه‌بندی سند ..... **عادی**

تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ به‌روزرسانی چندین آسیب‌پذیری در سیستم مدیریت محتوای دروپال

سیستم مدیریت محتوا دروپال(Drupal) به‌روزرسانی امنیتی را برای رفع چندین آسیب‌پذیری مختلف در نسخه‌های 7.x، 8.8.x، 8.9.x و 9.0.x منتشر کرده است. نفوذگران با بهره‌برداری از این آسیب‌پذیری‌ها می‌توانند اطلاعات حساسی را کسب کرده یا حمله تزریق کد (Cross-site scripting) انجام دهند. در جدول زیر لیست آسیب‌پذیری‌های رفع شده نمایش داده شده است.

لیست آسیب‌پذیری‌های به‌روزرسانی شده

شناسه آسیب‌پذیری	نوع آسیب‌پذیری	شدت آسیب‌پذیری	توصیف آسیب پذیری
CVE-2020-13666	تزریق کد	Moderately critical	عدم غیرفعال‌سازی JSONP به صورت پیش‌فرض در AJAX API دروپال موجب حملات تزریق کد می‌شود.
CVE-2020-13667	دور زدن دسترسی (Bypass Access)	Moderately critical	ماژول Experimental Workspaces امکان ایجاد چندین فضای‌کاری آزمایشی را فراهم آورده و به کاربران این اجازه را می‌دهد تا محتوای پیش‌نویس را قبل از انتشار در فضای‌کاری اصلی ویرایش نمایند. عدم کنترل کامل دسترسی‌ها در زمان سویچ بین Workspacesها منجر به آسیب‌پذیری دور زدن دسترسی می‌شود. بنابراین ممکن است نفوذگران بتوانند محتوایی را قبل از انتشار در سایت مشاهده نمایند. توجه به این نکته ضروریست تنها سایت‌هایی که ماژول Experimental Workspaces را نصب کرده‌اند، تحت تاثیر این آسیب‌پذیری قرار دارند.

CVE-2020-13668		Critical	نسخه‌های 8 و9 از دروپال در شرایط خاص دارای آسیب‌پذیری Reflected XSS هستند.
CVE-2020-13669	تزریق کد	Moderately critical	متد image caption در ویرایشگر داخلی دروپال (CKEditor) دارای آسیب‌پذیری XSS است.
CVE-2020-13670	افشای اطلاعات	Moderately critical	آسیب‌پذیری موجود در ماژول File به نفوذگران اجازه دسترسی به فراداده فایل‌های خصوصی را می‌دهد که در حال عادی با حدس شناسه فایل نمی‌توانستند به این اطلاعات دسترسی یابند.

راهکار مقابله با این آسیب‌پذیری‌ها نصب به‌روزترین نسخه موجود می‌باشد.

- اگر از نسخه 8.8.x دروپال استفاده می‌کنید به نسخه 8.8.10 به‌روزرسانی نمایید.
- اگر از نسخه 8.9.x دروپال استفاده می‌کنید به نسخه 8.9.6 به‌روزرسانی نمایید.
- اگر از نسخه 9.0.x دروپال استفاده می‌کنید به نسخه 9.0.6 به‌روزرسانی نمایید.

نسخه‌های پیش از نسخه 8.8.x دیگر پشتبانی نمی‌شوند و وصله امنیتی برای آن‌ها ارائه نشده است. در سایت‌های دارای نسخه 8.7.x یا نسخه‌های قدیمی‌تر از این نسخه ضروری است که سیستم مدیریت محتوا به نسخه 8.8.10 ارتقاء یابد.

در سه آسیب‌پذیری CVE-2020-13666، CVE-2020-13667 و CVE-2020-13668 علاوه بر به‌روزرسانی هسته سیستم مدیریت محتوا دروپال نیاز است تا مراحلی دیگری نیز برای اطمینان از رفع کامل آسیب‌پذیری در سایت انجام شود.

برای رفع آسیب‌پذیری CVE-2020-13668 در سایت‌هایی که متدهای buildFormAction() و renderPlaceholderFormAction() از Drupal\Core\Form\FormBuilder\را در کدهای اعانه (Contrib) و سفارشی (Custom) خود بازنویسی کرده‌اند، ضرویست اطمینان حاصل شود که پاک‌سازی (sanetizing) لازم برروی Urlها انجام شده است.

برای رفع آسیب‌پذیری CVE-2020-13666 اگر از AJAX API برای درخواست JSONP در سایت خود استفاده کرده باشید؛ در این صورت باید تنظیمات Ajax را به "jsonp: true" تغییر دهید یا از jQuery AJAX

API به صورت مستقیم استفاده کنید. همچنین در صورتی که از jQuery AJAX API برای Urlهای فراهم شده توسط کاربر در ماژول‌های اعانه و سفارشی استفاده می‌کنید باید کد خود را مرورکرده و هرجایی که لازم بود "jsonp: false" را تنظیم کنید.

بعلاوه باید دانست که این آسیب‌پذیری نسخه 7 سیستم مدیریت محتوای دروپال را نیز تحت تاثیر قرار می‌دهد و برای رفع این آسیب‌پذیری در این نسخه ضروری است که در گام اول سیستم مدیریت محتوا به نسخه 7.73 ارتقاء یابد. همچنین در این نسخه (نسخه 7 سیستم مدیریت محتوا دروپال) برای رفع آسیب‌پذیری احتمالی Urlهای فراهم شده باید این Urlها در تابع Drupal.sanitizeAjaxUrl() بررسی شوند.

باید توجه کرد که کاربران سایت‌هایی‌که ماژول experimental Workspaces در آن‌ها استفاده شده است حتی بعد از به‌روزرسانی نیز تا زمانی که از سیستم خارج نشده‌اند، می‌توانند به محتوای منتشر نشده که به دلیل آسیب‌پذیری در دسترس آن‌ها قرار داشت، دسترسی یابند. بنابراین در صورتی که توقف فوری دسترسی‌های ناخواسته ضروری باشد باید تمام جلسات کابران فعال سایت پایان یابد. برای مثال می‌توان جدول sessions را خالی کرد. البته باید توجه کرد که این کار موجب خروج فوری همه کاربران خواهد شد و دارای اثرات جانبی از جمله از دست رفتن اطلاعات وارد شده توسط کاربران می‌باشد.

منابع

https://us-cert.cisa.gov/ncas/current-activity/2020/09/17/drupal-releases-security-updates
https://www.waterisac.org/portal/drupal-releases-security-updates-0
https://www.drupal.org/project/drupal/releases