بسمه تعالی

حملات فعال به بیش از یک میلیون سایت وردپرسی

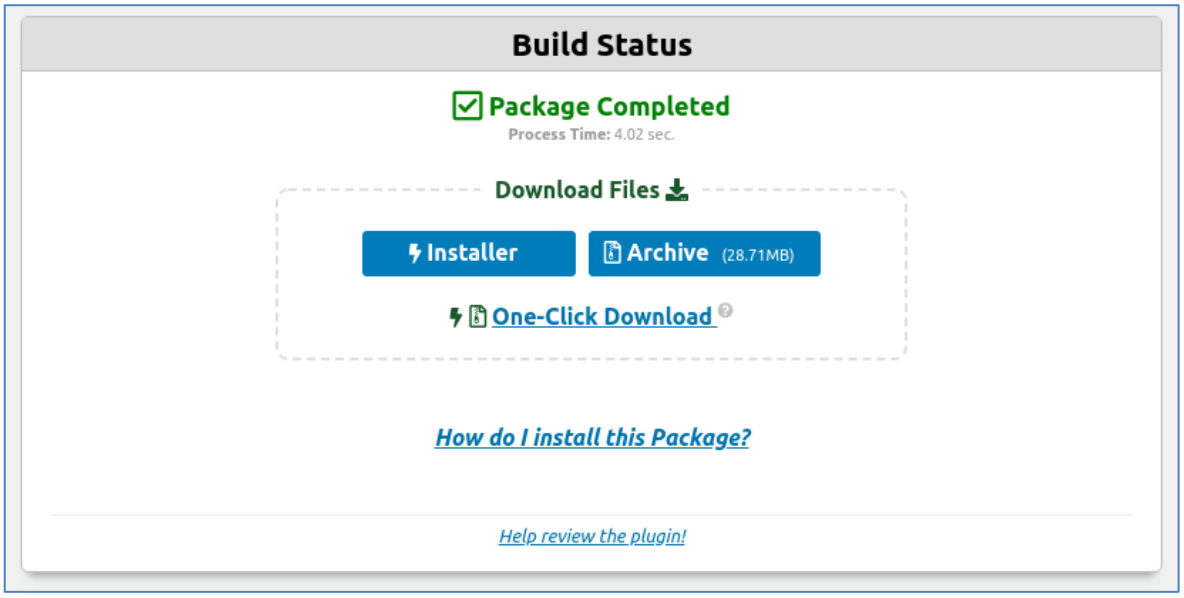
از طریق آسیب‌پذیری افزونه Duplicator

گزارش آسیب‌پذیری

یک آسیب‌پذیری بحرانی با درجه حساسیت مهم در یکی از معروف‌ترین افزونه‌های وردپرسی به نام Duplicator یافت شده است. بیش از یک میلیون سایت وردپرسی تحت تاثیر این آسیب‌پذیری که به مهاجم اجازه‌ی دانلود فایل دلخواه از وب‌سایت قربانی را می‌دهد، قرار دارند. در این گزارش به بررسی قطعات کد آسیب‌پذیر، اهمیت آن و جزییات حملات در حال انجام توسط این آسیب‌پذیری می‌پردازیم.

۱ تحلیل آسیب‌پذیری «دانلود فایل»

با استفاده از افزونه‌ی Duplicator امکان انتقال وب‌سایت و یا تهیه پشتیبان از آن برای آدمین سایت وردپرسی فراهم می‌شود. قسمتی از این عملکرد شامل برون‌ریزی[۱] پایگاه داده و محتوای فایل‌ها است. همان طور که شکل زیر مشاهده می‌شود، بعد از تهیه پشتیبان از وب‌سایت با استفاده از افزونه Duplicator، افزونه امکان دانلود فایل‌های تولید شده را در داشبورد WordPress فراهم می‌کند.



شکل شماره ۱ :امکان دانلود پشتیبان تهیه شده توسط افزونه Duplicator

این عملکرد از طریق یک درخواست AJAX در رابط آدمین افزونه، پیاده‌سازی شده است. هر دکمه دانلود، یک فراخوانی به WordPress AJAX handler را به وسیله‌ی تابع duplicator_download() و پارامتر ورودی

[۱] export

که موقعیت فایلی که دانلودی را نشان می‌دهد، آغاز می‌کند. به محض کلیک، فایل درخواست شده توسط کاربر بدون نیاز به ترک صفحه یا بارگذاری مجدد آن دانلود می‌شود.

```
public static function duplicator_download() {
        $file = sanitize_text_field($_GET['file']);
        $filepath = DUPLICATOR_SSDIR_PATH.'/'.$file;
        // Process download
        if(file_exists($filepath)) {
            // Clean output buffer
            if (ob_get_level() !== 0 && @ob_end_clean() === FALSE) {
                @ob_clean();
            }

            header('Content-Description: File Transfer');
            header('Content-Type: application/octet-stream');
            header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
            header('Expires: 0');
            header('Cache-Control: must-revalidate');
            header('Pragma: public');
            header('Content-Length: ' . filesize($filepath));
            flush(); // Flush system output buffer

            try {
                $fp = @fopen($filepath, 'r');
                if (false === $fp) {
                    throw new Exception('Fail to open the file '.$filepath);
                }
                while (!feof($fp) && ($data = fread($fp, DUPLICATOR_BUFFER_READ_WRITE_SIZE)) !== FALSE) {
                    echo $data;
                }
                @fclose($fp);
            } catch (Exception $e) {
                readfile($filepath);
            }
            exit;
        } else {
            wp_die('Invalid installer file name!!');
        }
    }
```

شکل شماره ۲: دانلود فایل مورد نظر از طریق تابع duplicator_download

تابع duplicator_dowload() توسط wp_ajax_nopriv_ ثبت شده است درنتیجه کاربران بدون نیاز به احراز هویت به این تابع دسترسی خواهند داشت. از طرفی هیچ نوع ارزیابی در مورد آدرس فایلی که درخواست دانلود آن داده شده است، صورت نمی‌گیرد. مطابق شکل بالا آدرس فایل دانلودی با DUPLICATOR_SSDIR_PATH آغاز می‌شود اما مهاجم با تغییر این آدرس به مقادیری مانند ../../../file.php می‌تواند ساختار فایلی سرور را بدست آورد.

آسیب پذیری مشابه‌ی در تابع duplicator_init() این افزونه وجود دارد که توسط تابع init متعلق به WordPress فراخوانی می‌شود. این فراخوانی موجب می‌شود تا تابع duplicator_init() با هر بار بازگذاری صفحه وب وردپرسی توسط کاربران احراز هویت شده (logged in) و یا احراز هویت نشده، اجرا شود. این به آن معنی است که مهاجم با دور زدن مانیتورینگ AJAX و اضافه کردن رشته‌های پرس‌وجو[۲] به هر آدرسی از پایگاه داده در سایت آسیب‌پذیر، می‌تواند دانلود فایل را آغاز کند.

---

[۲] query

```php
function duplicator_init() {
    if (isset($_GET['action']) && $_GET['action'] == 'duplicator_download') {
        $file = sanitize_text_field($_GET['file']);
        $filepath = DUPLICATOR_SSDIR_PATH.'/'.$file;
        // Process download
        if(file_exists($filepath)) {
            // Clean output buffer
            if (ob_get_level() !== 0 && @ob_end_clean() === FALSE) {
                @ob_clean();
            }

            header('Content-Description: File Transfer');
            header('Content-Type: application/octet-stream');
            header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
            header('Expires: 0');
            header('Cache-Control: must-revalidate');
            header('Pragma: public');
            header('Content-Length: ' . filesize($filepath));
            flush(); // Flush system output buffer

            try {
                $fp = @fopen($filepath, 'r');
                if (false === $fp) {
                    throw new Exception('Fail to open the file '.$filepath);
                }
                while (!feof($fp) && ($data = fread($fp, DUPLICATOR_BUFFER_READ_WRITE_SIZE)) !== FALSE) {
                    echo $data;
                }
                @fclose($fp);
            } catch (Exception $e) {
                readfile($filepath);
            }
            exit;
        } else {
            wp_die('Invalid installer file name!!');
        }
    }
}
add_action('init', 'duplicator_init');
```

شکل شماره ۳: duplicator_init() که توسط تابع init خود WordPress فراخوانی می‌شود

هر دو مورد آسیب‌پذیری در نسخه ۱.۳.۲۸ افزونه بر طرف شده است به طوری که ارزیابی‌های لازم در خصوص آدرس فایلی که دانلود خواهد شد با استفاده از یک شناسه و هش متناظر با آن صورت می‌گیرد. همچنین تابع duplicator_init() نیز بطور کلی حذف شده است.

۲ سرقت اعتبارنامه‌های پایگاه داده توسط مهاجمان

آسیب‌پذیری «دانلود فایل دلخواه» در هر نوع سایتی بسته به پلتفرم آن مخاطره‌آمیز است اما در مورد سایت‌های وردپرسی فایلی به نام wp-config.php مورد توجه ویژه‌ی مهاجمان خواهد بود؛ جایی که اعتبارنامه‌های پایگاه داده نگهداری می‌شود. با استفاده از این اعتبارنامه‌ها و فعال بودن امکان اتصال از راه دور به پایگاه داده، مهاجم می‌تواند مستقیماً به پایگاه داده سایت قربانی متصل شود. این اتصال می‌تواند به منظور ساخت یک حساب کاربری آدمین برای آسیب زدن به وب‌سایت در آینده، تزریق اطلاعات و یا سرقت آن انجام گیرد.

طبق گزارش Wordfence بیش از ۶۰.۰۰۰ تلاش مبنی بر دانلود فایل wp-config.php سایت‌های وردپرسی صورت گرفته که ۵۰.۰۰۰ تلاش قبل از برطرف شدن این آسیب‌پذیری است. تقریبا همه‌ی این تلاش‌ها از یک آدرس IP یکسان 77.71.115.52 که مربوط به وب سروری در بلغارستان متعلق به Varna Data Center EOOD می‌باشد، صورت گرفته است.

۳ علائم آسیب‌پذیری (IOCs)

موارد زیر می‌تواند نشان‌دهنده‌ی حمله‌ی احتمالی به وبسایت باشد:

- ترافیک ثبت شده از آدرس IP: 77.71.115.52
- حملات این کمپین با استفاده از درخواست‌های GET و رشته پرس‌وجوهای زیر صورت می‌گیرد:
  - action=duplicator_download
  - file=/../wp-config.php

به همه‌ی کاربران این افزونه توصیه می‌شود تا در اسرع وقت به به‌روزرسانی افزونه به نسخه ۱.۳.۲۸ اقدام کنند.

همچنین چنانچه متوجه حمله به وب‌سایت خود شدید هرچه سریع‌تر به تغییر اعتبارنامه‌های پایگاه داده اقدام کنید.

۴ مراجع

[۱] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-on-prem-static-cred-sL8rDs8