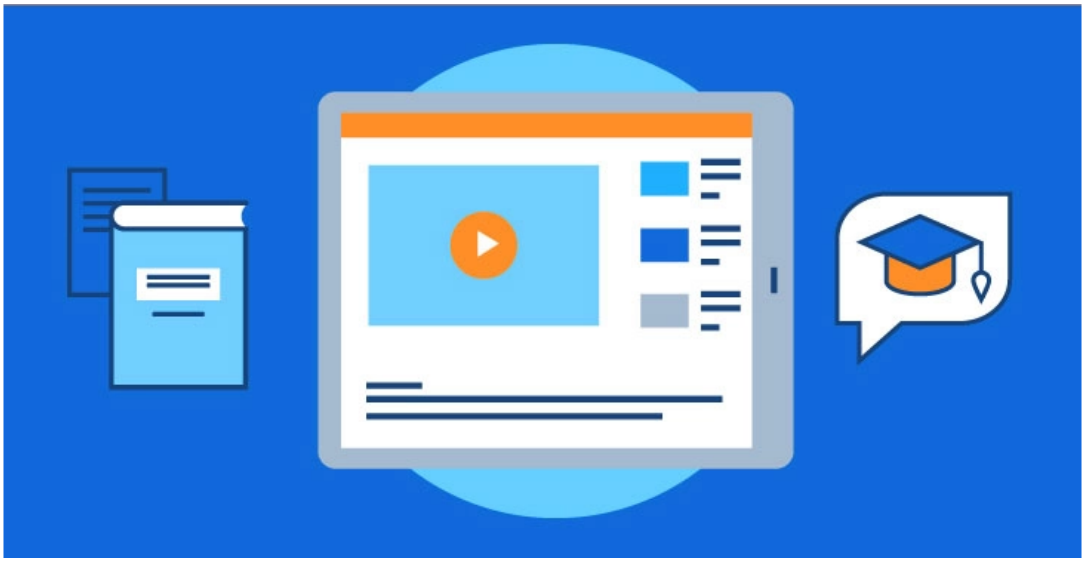
بسمه تعالی

عنوان خبر:

کشف نقص بحرانی در سه افزونه‌ی e-Learning محبوب وردپرس

گروه خبری:

آسیب‌پذیری



محققان امنیتی در خصوص آسیب‌پذیری جدیدِ در برخی از افزونه‌های محبوب سیستم‌های مدیریت آموزش آنلاین[1](LMS) به کاربران هشدار دادند. به گفته‌ی تیم تحقیقاتی Check Point سه افزونه[2] وردپرس LearnPress, LearnDash و LifterLMS دارای نقص امنیتی می‌باشند به طوری که به دانشجویان و همچنین کاربران غیرمجاز اجازه می‌دهند تا اطلاعات شخصی کاربران ثبت شده را به سرقت برده و حتی به امتیاز و سطح دسترسی معلمان نیز دست یابند. سازمان‌ها و دانشگاه‌های بسیاری جهت برگزاری دوره‌های آموزش آنلاین از طریق وب سایت‌های مبتنی بر وردپرس، از این سیستم‌ها استفاده می‌کنند.

Omri Herscovici که یکی از محققان Check Point می‌باشد اذعان داشت: "به دلیل شیوع ویروس کرونا، ناچار به یادگیری از راه دور و از طریق فضای مجازی هستیم و از طرفی نیز آسیب‌پذیری‌های کشف شده به دانشجویان و حتی به کاربران غیرمجاز اجازه می‌دهد تا اطلاعات حساسی را بدست آورده و یا کنترل پلتفرم‌های LMS را به دست گیرند."

سه سیستم LMS نام برده، حدوداً بر روی ۱۰۰،۰۰۰ پلتفرم آموزشی دانشگاه‌های مختلف از جمله دانشگاه‌های فلوریدا، میشیگان و واشنگتن نصب شده‌اند و LearnPress وLifterLMS نیز از زمان انتشارشان به تنهایی بیش از ۱٫۶ میلیون بار دانلود شده‌اند.

LMS از طریق اپلیکیشن‌های مختلف، امر یادگیری آنلاین را برای کاربران تسهیل بخشیده و از این طریق مؤسسات آموزشی می‌توانند برنامه‌های درسی مختص خود را ایجاد کنند، آن‌ها را به اشتراک بگذارند، دانش‌آموزان را ثبت‌نام و آن‌ها را طریق برگزاری آزموهای مختلف ارزیابی کنند، افزونه‌های کاربردی LearnPress، LearnDash و LifterLMS نیز با تطبیق هر سایت وردپرس با یک LMS کارآمد، توانسته‌اند این امر را آسان نمایند.

[1] learning management system
[2] plugin

```
function learn_press_accept_become_a_teacher() {
  $action  = ! empty( $_REQUEST['action'] ) ? $_REQUEST['action'] : '';
  $user_id = ! empty( $_REQUEST['user_id'] ) ? $_REQUEST['user_id'] : '';
  if ( ! $action || ! $user_id || ( $action != 'accept-to-be-teacher' ) ) {
    return;
  }

  if ( ! learn_press_user_maybe_is_a_teacher( $user_id ) ) {
    $be_teacher = new WP_User( $user_id );
    $be_teacher->set_role( LP_TEACHER_ROLE );
    delete_transient( 'learn_press_become_teacher_sent_' . $user_id );
    do_action( 'learn_press_user_become_a_teacher', $user_id );
    $redirect = add_query_arg( 'become-a-teacher-accepted', 'yes' );
    $redirect = remove_query_arg( 'action', $redirect );
    wp_redirect( $redirect );
  }
}
add_action( 'plugins_loaded', 'learn_press_accept_become_a_teacher' );
```

نقص موجود در افزونه‌ی LearnPress، قادر به انجام حمله‌ی تزریق کد SQL (با شناسه‌ی CVE-۲۰۲۰-۶۰۱۰) و افزایش سطح دسترسی کاربر به سطح معلم (با شناسه‌ی CVE-۲۰۲۰-۶۰۱۱) می‌باشد.

محققان اظهار داشتند که: "کد مذکور، مجوزهای دسترسی را برای کاربران مختلف بررسی نخواهد کرد، بنابراین به هر دانش‌آموزی مجوز انجام هر کاری را خواهد داد."

به همین ترتیب آسیب‌پذیری موجود در افزونه‌ی LearnDash (با شناسه‌ی CVE-۲۰۲۰-۶۰۰۹) نیز با استفاده از شبیه‌ساز سرویس مسیجِ PayPal's Instant Payment Notification(IPN)، کد SQL مخرب را تزریق کرده و زمینه را برای ثبت‌نام دوره‌های جعلی آماده خواهد کرد.

نقص موجود در افزونه‌ی LifterLMS (با شناسه‌ی CVE-۲۰۲۰-۶۰۰۸) نیز از ماهیت اپلیکیشن‌های PHP سوءاستفاده کرده و به مهاجم اجازه می‌دهد تا تنها با یک قطعه کد مخرب PHP، نام پروفایل خود را تغییر دهد (به عنوان مثال، دانشجویی که برای دوره‌ی خاصی ثبت‌نام کرده است).

در نهایت این نقص‌ها باعث می‌شود تا مهاجمان بتوانند اطلاعات شخصی کاربران (مانند: نام، ایمیل، نام‌کاربری، گذرواژها و غیره) را به سرقت برده و دانش آموزان نیز بتوانند نمرات را تغییر دهند، سوالات آزمون‌های مختلف و پاسخ‌های آن‌ها را از قبل بدست آورند و همچنین قادر خواهند بود که گواهی‌نامه‌ها را جعل کنند.

محققان هشدار دادند که این پلتفرم‌ها شامل درگاه پرداخت بوده و مهاجم می‌تواند بدون اطلاع کاربر از طریق آسیب‌پذیری‌های مذکور، از طرح‌های مالی سوءاستفاده کند.

به گفته‌ی Check Point Research این آسیب‌پذیری‌ها در ماه مارس سال ۲۰۲۰ کشف شدند و برای هر یک از سیستم‌های LMS نام برده، وصله‌های امنتی منتشر شده است و به کاربران توصیه شود حتماً از نسخه‌های
آپدیت این افزونه‌ها استفاده کنند.

منبع خبر:

https://thehackernews.com/۲۰۲۰/۰۴/wordpress-lms-plugins.html