بولتن تحلیلی ■ دی ماه ۱۳۹۸

امنیت اطلاعات

پادویش
Padvish

بولتن تحلیلی امنیت اطلاعات،
تهیه شده توسط پادویش

پیش‌گفتار

در خبرنامه دی ماه ۹۸ پادویش، به تازه‌ترین اخبار منتشر شده در حوزه امنیت و رویدادهای بدافزاری خواهیم پرداخت.

درابتدای این خبرنامه، به یکی از موضوعات و دغدغه‌های روز کاربران شبکه‌های مجازی از جمله اینستاگرام، در ارتباط با امنیت اطلاعات می‌پردازیم و یکی از خانواده‌های بدافزاری فعال اینستاگرامی را معرفی خواهیم کرد.

در ادامه، به بدافزارهای ماینری و نقش آنها در آلودگی‌های بدافزاری سال‌های اخیر می‌پردازیم. همچنین یکی از ماینرهای مشاهده شده در سیستم کاربران ایرانی توسط پادویش و راهکارهای پیشنهادی برای مقابله با این نوع بدافزار را معرفی خواهیم کرد.

در انتها نیز به اصلاحیه‌های منتشر شده از سوی شرکت‌های نرم‌افزاری شناخته شده، در دی ماه ۹۸ اشاره می‌کنیم.

شرکت نرم‌افزاری امن پرداز، تولید کننده‌ی آنتی ویروس پادویش، با هدف گسترش امنیت در حوزه‌ی فناوری اطلاعات و فضای مجازی، با انتشار اخبار روز در این حوزه، سعی در آگاهی بخشی مخاطبان دارد. امیدواریم خبرنامه پیش رو و سایر گزارش‌های آتی از سوی گروه فنی و انتشار محتوای پادویش، مورد استفاده کاربران محترم قرارگیرد.

حملات بدافزاری در کمین کاربران اینستاگرام

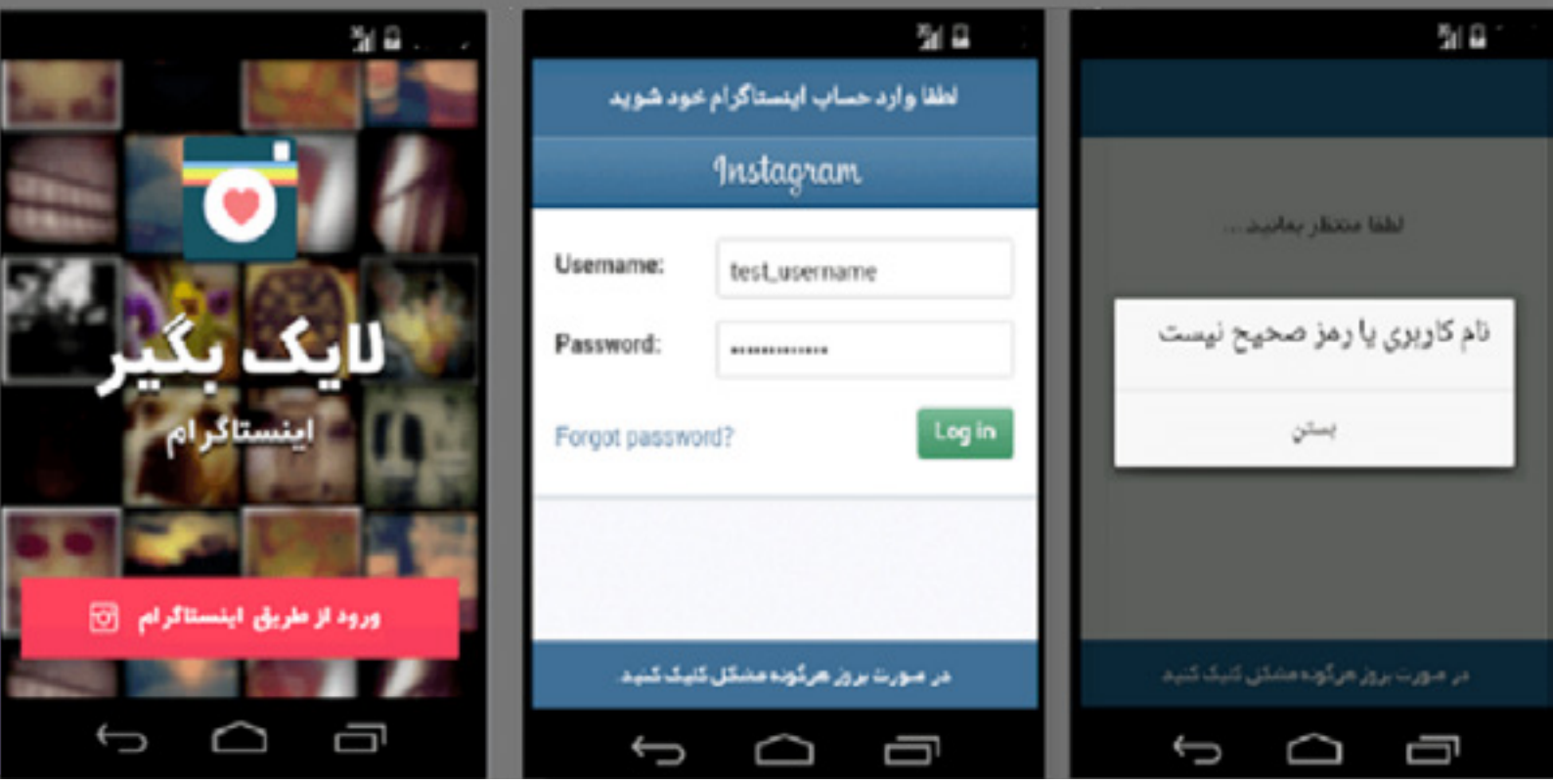
این روزها بحث امنیت در اینستاگرام، بین کاربران ایرانی بسیار داغ است. بسیاری از صفحه‌های پر بازدید و بلاگرهای معروف اینستاگرام، از کمک افراد متخصص در زمینه شبکه، در جهت تامین امنیت خود استفاده می‌کنند. اما مفهومی به نام امنیت در اینستاگرام تا چه حد جدی است و آیا کاربران، به تنهایی قادر به حفاظت اطلاعات خود هستند یا خیر.

در سال‌های اخیر و پس از ظهور اینستاگرام، بسیاری از هکرها با هدف سرقت اطلاعات کاربران، اقدام به طراحی بدافزارهای اینستاگرامی کرده‌اند. سازوکار هر یک از آنها شکل مخصوص به خود را دارد و نمی‌توانیم همگی را در دسته‌ای خاص بگنجانیم. در اینجا قصد داریم تا به معرفی سازوکار یکی از این خانواده‌های بدافزاری که با هدف فیشینگ، اطلاعات کاربران را به سرقت می‌برند، بپردازیم.

نحوه آلوده شدن کاربران به این دسته از بدافزارها که از حملات فیشینگ استفاده می‌کنند، معمولا از طریق تبلیغات این برنامه‌های آلوده در کانال‌های تلگرامی و یا اینستاگرام می‌باشد. اغلب این برنامه‌ها دارای پرداخت درون برنامه‌ای هستند. هرگونه تلاش جعلی برای به دست آوردن اطلاعات حساس مانند اطلاعات کارت‌های بانکی، اطلاعات حساب کاربری یا سایر اطلاعات شناسایی شخصی، جزو حملات فیشینگ محسوب می‌شود. به عبارت دیگر، هکرها برای به دست آوردن اطلاعات حساب بانکی، یک صفحه‌ی پرداخت مانند صفحه‌ی پرداخت بانکی ایجاد می‌کنند و آن را جایگزین صفحه اصلی پرداخت بانک می‌کنند.

در این نوع حملات، با روشی خاص شما وارد صفحه‌ی پرداخت جعلی می‌شوید و اطلاعات حساب کاربریتان درخواست می‌شود. در واقع اینجاست که سرقت اطلاعات رخ داده است و کاربر با وارد کردن مشخصات خود و با زدن دکمه ارسال، اطلاعات را به سمت مهاجم ارسال می‌کند. برنامه‌های بسیار زیادی با همین منظور طراحی شده‌اند که معمولا برای جذب مخاطب بیشتر، از نام‌های فریبنده مانند وعده خرید شارژ نصف قیمت و یا بازی‌هایی با نام‌های مستهجن استفاده می‌کنند.

در ادامه یکی از شایع‌ترین بدافزارهای اینستاگرامی در ایران، به نام خانواده‌ی FakeGram را تحلیل و بررسی خواهیم کرد.



FakeGram؛ سارق حرفه‌ای اطلاعات اکانت اینستاگرام

بدافزار جاسوسی FakeGram نام خانواده‌ای از بدافزارهاست که با وعده جذب فالوور، لایک یا کامنت بیشتر، سعی در سرقت اطلاعات حساب کاربری قربانیان دارد. با محبوبیت روزافزون شبکه‌ی اجتماعی اینستاگرام و تمایل کاربران به افزایش مخاطب، شهرت و یا درآمد بیشتر، با رشد سریع این دسته از بدافزارها نیز مواجه بوده‌ایم. این برنامه‌ها که به شکل انبوهی در مارکت‌های اندرویدی مانند کافه بازار یافت می‌شوند، با طراحی برنامه‌های آلوده خود مشابه صفحه اصلی اینستاگرام، کاربران بسیاری را جذب می‌کنند. اما در پس این ظاهر فریبنده، مهاجمان در کمین اطلاعات حساب کاربری قربانیان مانند آدرس ایمیل و کلمه عبور هستند.

سایر برنامه‌های آلوده به این نوع بدافزار شامل ادبین (بازدید بگیر سایت و لینک)، لایک بگیر اینستاگرام، فالوئر بگیر اینستاگرام، آیدی لیست، کامنت بگیر اینستاگرام، عضو در عضو، اینستا استار می‌باشند.

عملکرد این بدافزارهای فیشینگ به این شکل است که با نمایش صفحه‌ای جعلی و مشابه صفحه لاگین اینستاگرام اطلاعات حساب کاربری قربانی، درخواست می شود. همچنین برای جلب اعتماد کاربران، از توضیحاتی جعلی مانند "نام کاربری و رمز عبور شما توسط ما قابل دسترسی نیست و شما مستقیم در Instagram لاگین می‌کنید" استفاده می‌شود. با ورود اطلاعات کاربری اینستاگرام، پیامی مبنی بر نادرست بودن رمز عبور نمایش داده می‌شود اما در این حین به وسیله کدهای جاوا اسکریپت پنهان که در پس زمینه در حال اجرا هستند، اطلاعات قربانی به مهاجمان ارسال می‌شود، تا از اکانت‌های به سرقت رفته در جهت منافع خود استفاده کنند. با ورود مهاجمان به حساب کاربری افراد، پیامی از سمت اینستاگرام با متن "اطلاعات شما از گوشی دیگری در حال لاگین شدن می‌باشد و این که آیا آن شخص خود شما هستید یا خیر" دریافت می‌شود. هدف اصلی این‌گونه بدافزارهای فیشینگ، جمع آوری اطلاعات کاربران اینستاگرام و نمایش تبلیغات می‌باشد که این تکنیک از مرسوم‌ترین روش‌های سودجویی از قربانیان است.

برای اطمینان خاطر از عدم آلودگی دستگاه، فایل پایگاه داده آنتی ویروس پادویش را بروز نگه دارید و اسکن آنتی ویروس را انجام دهید. همچنین توصیه می‌شود رمز ورود اینستاگرام و همچنین جزئیات ورود خود را در هر وب سایت دیگری که برای آن از همان ترکیب ایمیل و رمز عبور استفاده کرده‌اید، تغییر دهید. به علاوه یکی دیگر از روش‌های مصون ماندن داده‌ها از سارقان فضای مجازی، دوری از نصب هر گونه برنامه مشکوکی است که با وعده‌های دروغین، برنامه‌ای مشابه با برنامه نسخه اصلی نصب می‌کنند.

استخراج‌کنندگان ارز دیجیتال؛ سارقان نامرئی منابع

ماینینگ یا استخراج

ماینینگ یا استخراج یک نوع فرایند رقابتی است که در حین انجام این فرایند، سیستم توسط استخراج‌کننده ارز دیجیتال و به منظور تایید تراکنش‌ها در اختیار شبکه قرار می‌گیرد. این فرایند سودآور، علیرغم تولید ارز دیجیتال، به منابع محاسباتی قابل توجهی نیاز دارد. معاملات در Blockchain که به عنوان یک دفترچه راهنمای عمومی کار می‌کند، ثبت می‌شوند. کامل بودن و انسجام Blockchain در وضعیتی تنظیم شده است که توسط استخراج‌کنندگان غیرقابل تغییر است و به محض انجام تراکنش‌های جدید، به طور مداوم تأیید می‌شود.

استخراج‌کنندگان ارز دیجیتال

استخراج‌کنندگان ارز دیجیتال یا ماینرها، برنامه‌هایی برای تولید و استخراج بیت کوین، مونرو، اتریوم یا سایر ارزهای دیجیتال می‌باشند. در صورتی که از استخراج‌کنندگان ارز دیجیتال در جهت منافع شخصی استفاده شود، منبع درآمد باارزشی به حساب می‌آیند. با این حال، تولیدکنندگان بدافزارها، تهدیدها و ویروس‌هایی ایجاد کرده‌اند که از نرم‌افزارهای متداول و در دسترس استخراج در جهت استفاده از توان محاسباتی سیستم اشخاص دیگر، بدون اطلاع و رضایت آنها استفاده می‌کنند. قسمت‌های بکار گرفته شده‌ی سیستم عبارت اند از: RAM، GPU، CPU ، پهنای باند شبکه و power.
مجرمان سایبری با اصلاح استخراج‌کنندگان ارز دیجیتال موجود و با استفاده از مکانیسم‌های پیچیده و نرم افزارهای مخرب یا حفره‌های امنیتی، اقدام به توزیع و نصب تروجان‌های استخراج‌کننده‌ی ارز دیجیتال بر روی کامپیوترهای قربانیان می‌کنند. جالب است بدانید که گسترش برنامه‌های مخرب استخراج ارز دیجیتال، با کاهش حجم باج افزارها همراه بوده است. حال این سوال مطرح می‌شود که آیا این دو روند با هم در ارتباط هستند و آیا مجرمان سایبری تمرکز خود را بر روی استخراج ارز دیجیتال به عنوان منبع اصلی درآمد خود تغییر می‌دهند یا خیر. احتمال اینکه مجرمان سایبری عملیات باج‌افزاری را به طور کامل متوقف کنند خیلی پایین است، اما افزایش قیمت بیت کوین علاقه‌ی روز افزونی را به ارزهای دیجیتال معطوف کرده است که چشم انداز امنیت سایبری را نیز تحت تاثیر قرار خواهد داد.
از زمانی که مجرمان سایبری از طریق باج افزارها شروع به درخواست باج در قالب ارز دیجیتال نمودند، هویت بدی را به ارزهای دیجیتال بخشیدند، که اولین و مهمترین این ارزها بیت کوین بود. علاوه بر این، ماهیت بینام ارزهای دیجیتال، هویت ناشناسی را که مجرمان سایبری به دنبال آن بودند تحقق بخشید و افزایش شدید ارزش بیت کوین در مدت زمانی کوتاه یک دستاورد باد آورده برای آنها بوده است.

انواع استخراج‌کنندگان ارز دیجیتال

انواع گوناگون استخراج‌کننده‌های ارز دیجیتال از کامپیوتر و یا سایر دستگاه‌ها وجود دارد که سه نوع اصلی آن عبارت‌اند از:

• اجرایی: این دسته، فایل‌های اجرایی معمولی مخرب یا برنامه‌های خاکستری هستند که برنامه‌های ناخواسته بالقوه (PUA) نیز نامیده می‌شوند و به منظور استخراج ارزهای دیجیتال از سیستم طراحی شده‌اند.

• استخراج‌کنندگان ارز دیجیتال مبتنی بر مرورگر: این استخراج‌کنندگان JavaScript (یا فناوری مشابه) کار خود را در یک مرورگر اینترنتی انجام می‌دهند و مادامی که مرورگر در وب سایت باز باقی بماند، منابع سیستم قربانی را مصرف می‌کنند. برخی مالکان وب سایت‌ها بجای اجرای تبلیغات، از استخراج‌کنندگان ارز دیجیتال استفاده می‌کنند (به عنوان مثال Coinhive)، در حالی که برخی دیگر (معمولاً سایت‌های پخش ویدئو) توسط مجرمان سایبری و به طور خاص برای اهداف استخراج تنظیم شده‌اند که بدون اطلاع و رضایت مالک وب سایت به وب سایت قانونی تزریق و هر یک در چندین لایه iframe پنهان می‌شوند.

• استخراج‌کنندگان ارز دیجیتال پیشرفته بدون فایل: بدافزارهایی که با استفاده نادرست از ابزارهای قانونی مانند PowerShell، کار استخراج ارز دیجیتال خود را بر روی حافظه کامپیوتر انجام می‌دهند. یک نمونه MSH.Bluwimps است که علاوه بر کار استخراج ارز دیجیتال، اقدامات مخرب دیگری را نیز انجام می‌دهد. تشخیص این دسته از بدافزارها به دلیل بدون فایل بودن بدافزار مشکل است. اغلب راه‌حل‌های متداول آنتی ویروس‌ها، توانایی تشخیص این بدافزارهای بدون فایل را ندارند و البته حذف دستی بدافزار نیز به مهارت فنی قابل توجهی احتیاج دارد.

نحوه انتشار استخراج‌کنندگان ارز دیجیتال

- ایمیل‌های حاوی پیوست‌های آلوده که سعی در نصب بدافزار دارند.

- وب‌سایت‌های میزبان کیت‌های اکسپلویت که سعی در استفاده از آسیب‌پذیری مرورگرهای وب و سایر نرم‌افزارها در جهت نصب استخراج‌کنندگان ارز دیجیتال دارند.

- وب‌سایت هایی که با اجرای اسکریپت‌هایی در هنگام استفاده کاربر از مرورگر، از قدرت پردازش کامپیوتر سوء استفاده می‌کنند.

- با بکارگیری یک آسیب‌پذیری خاص به نام Eternal blue در همه سیستم‌های ویندوزی پخش می‌شوند.

چگونه متوجه شوم که از سیستم من برای استخراج ارز دیجیتال استفاده می‌شود یا خیر؟

استخراج‌کنندگان ارز دیجیتال روی بسترهای مختلفی اجرا می‌شوند، از جمله: Android، Linux، Mac، Windows، دستگاه های اینترنت اشیاء (IoT)

علائم آلودگی به بدافزارهای استخراج کننده ارز دیجیتال

• بکارگیری زیاد CPU و GPU
• گرمای بیش از حد
• خرابی یا restart شدنهای متعدد
• زمان پاسخ آهسته
• فعالیت غیرمعمول شبکه (مانند اتصال به وب سایت‌ها و IP های مرتبط با استخراج ارز دیجیتال)

راهکارهای اولیه پس از شناسایی آلودگی

برگه مرورگری که URL شناسایی شده در آن باز است، ببندید. همچنین لازم است از بازدید وب‌سایتهای شناسایی شده خودداری کنید. برنامه یا فایل مخرب احتمالی شناسایی شده باید از کامپیوتر شما حذف شود. بنابراین پیش از حذف، از اجرای برنامه آلوده خودداری کنید.

نحوه محافظت در برابر استخراج‌کنندگان ارز دیجیتال

فعال کردن تشخیص PUA و Windows Defender ATP: برخی از ابزارهای استخراج ارز دیجیتال بدافزار محسوب نمی‌شوند اما به عنوان برنامه‌های ناخواسته بالقوه (PUA) شناسایی می‌شوند. بسیاری از برنامه‌های شناسایی شده به عنوان PUA می‌توانند بر عملکرد دستگاه و بهره وری آن تأثیر منفی بگذارند. در محیط‌های سازمانی، در صورتی که از آنتی ویروس‌های قدرتمند برای جلوگیری از نفوذ این بدافزارها استفاده نمی‌کنید، با فعال کردن این قابلیت‌ها میتوانید برخی از ابزارهای تبلیغاتی مزاحم و استخراج ارز دیجیتال را متوقف کنید.

در ادامه به تحلیل یکی از بدافزارهای ماینری یافت شده در میان کاربران ایرانی خواهیم پرداخت.

بدافزار Slytherin

Slytherin متعلق به خانواده بزرگ ماینرهاست. این برنامه‌ی مخرب با هدف استخراج ارز دیجیتال وارد سیستم می‌شود و با بهره‌برداری از آسیب‌پذیری‌های مختلف و همچنین دانلود سایر فایل‌های مخرب، سیستم و شبکه قربانی را آلوده می‌کند.

بکارگیری پردازه‌های سیستمی و توان محاسباتی کامپیوتر از اولین نشانه‌های حضور ماینر در سیستم قربانی است که کندی سیستم را به دنبال خواهد داشت.

Slytherin با اتصال به لینک مشخصی با آدرس http://sql.۴i۷i.com اقدام به دانلود سایر بدافزارهایی که قادر به انجام اقدامات مخرب موردنظر هستند، می‌کند. از آنجایی که Slytherin از دسترسی سطح بالایی برخوردار است، با بررسی وجود آنتی ویروس در سیستم و پاک کردن سرویس‌های موجود، راه را برای خود هموار می‌کند. سپس با تغییر در مقادیر موجود در رجیستری، امکان دسترسی ریموت دسکتاپ را برای سایر کاربران شبکه فراهم می‌آورد.

مؤثرترین روش مقابله با اینگونه بدافزارها، تشخیص به هنگام و جلوگیری از نفوذ آنها، پیش از آلودگی سیستم است.

بکارگیری دیوار آتش آنتی‌ویروس پادویش، از وقوع حملات شبکه‌ای توسط این دسته از بدافزارها جلوگیری و همچنین فایل js بدافزار را شناسایی می‌کند. ازاین‌رو جهت پیشگیری از آلودگی پیشنهاد می‌شود با نصب پادویش از ورود بدافزار به سیستم خود جلوگیری کنید.

اصلاحیه‌های منتشر شده در دی ماه 98

همچون ماه‌های گذشته، در دی ماه نیز شرکت‌های نرم افزاری مختلف اقدام به انتشار آسیب‌پذیری‌های یافت شده در سیستم‌های خود و اصلاحیه‌های مرتبط با آنها کردند. در ادامه به توضیح مختصری درباره اصلاحیه‌های امنیتی شرکت‌های Adobe، Cisco و گوگل خواهیم پرداخت. جهت مطالعه جزئیات بیشتر هر یک از این آسیب‌پذیری‌ها و دریافت اصلاحیه‌های مربوطه، می‌توانید به وب‌سایت خبری امن‌پرداز و لینک‌های موجود در هر یک مراجعه نمایید.

بروزرسانی‌های امنیتی Adobe در دسامبر ۲۰۱۹

• بروزرسانی‌های امنیتی برنامه Adobe Acrobat and Reader

نرم افزار Adobe Acrobat and Reader برنامه‌ای مطمئن برای مشاهده، چاپ و یادداشت‌گذاری در اسناد پی دی اف است. در ماه دسامبر، شرکت Adobe بروزرسانی‌های امنیتی جدیدی برای این برنامه در نسخه‌های ویندوز و مک ارائه داده است. این بروزرسانی‌ها شامل آسیب پذیری‌های بحرانی و مهمی است که در صورت سوءاستفاده موفق، امکان اجرای کد دلخواه را در برنامه کاربر فراهم می‌آورد.

• بروزرسانی امنیتی برنامه ColdFusion

شرکت Adobe زبان برنامه‌نویسی داینامیکی برای تولید برنامه‌های کاربردی وب سایت‌ها طراحی کرده است که به منظور میزبانی از این وب سایت‌ها نیاز به سرور وب ColdFusion می‌باشد. ColdFusion یک محیط توسعه مبتنی بر Eclipse است که برنامه نویسان ColdFusion را قادر می‌سازد پروسه کامل طراحی Web Application ها را از مفهوم تا پیاده‌سازی مدیریت نمایند. بروزرسانی‌های ماه دسامبر، مربوط به نسخه ۲۰۱۸ این برنامه است که آسیب‌پذیری‌های مهمی که منجر به افزایش امتیاز می‌شود را بر طرف کرده است.

• بروزرسانی امنیتی برنامه Brackets

Brackets یک برنامه ویرایشگر کد است که تمرکز اصلی آن توسعه وب می‌باشد. این برنامه ساخت شرکت Adobe و نرم‌افزاری متن باز و رایگان می‌باشد. شرکت Adobe بروزرسانی امنیتی جدیدی از این برنامه برای نسخه‌های ویندوز، مک و لینوکس را منتشر کرده است. این بروزرسانی شامل آسیب‌پذیری بحرانی است که در صورت سوءاستفاده موفق، امکان اجرای کد دلخواه را در برنامه کاربر فراهم می‌آورد.

• بروزرسانی‌های امنیتی برنامه Adobe Photoshop CC

برنامه Photoshop CC با دارا بودن کاربردهای متعدد، از ویرایش‌های روزمره گرفته تا تغییرات کلی به عنوان یکی از محبوب‌ترین محصولات شرکت Adobe محسوب می‌شود. از تغییر، برش و ویرایش عکس گرفته تا طراحی وب سایت و برنامه‌های تلفن همراه و یا ایجاد آثار هنری سه بعدی و فیلم، همگی از کاربردهای این برنامه بی‌نظیر هستند. شرکت Adobe بروزرسانی امنیتی جدیدی از این برنامه برای نسخه‌های ویندوز و مک را منتشر کرده است. این بروزرسانی شامل چندین آسیب‌پذیری بحرانی است که در صورت سوءاستفاده موفق، امکان اجرای کد دلخواه را در برنامه کاربر فراهم می‌آورد.

بروزرسانی‌های امنیتی سیسکو در دسامبر ۲۰۱۹

این اصلاحیه‌ها شامل ۳ مورد با درجه اهمیت بالا و ۲ مورد با اهمیت متوسط هستند. در ادامه به اولین آسیب‌پذیری برطرف شده اشاره می‌کنیم:

• آسیب‌پذیری اجرای کد از راه دور محصولات Adaptive Security Appliance و Firepower Threat Defense

آسیب‌پذیری در هنگام اجرای مفسر Lua که در نرم‌افزارهای امنیتی و محافظتی Cisco ادغام شده است، به مهاجمان اجازه دسترسی از راه دور برای اجرای کد دلخواه خود و با امتیازات اصلی در سیستم عامل لینوکس دستگاه آسیب‌دیده را فراهم می‌کند. مفسر Lua، مفسر مستقلی است که برنامه‌های Lua را چه به صورت منبع متنی و چه به صورت باینری از پیش جمع شده بارگیری و اجرا می‌کند. Lua را هم می توان به عنوان یک مترجم batch و هم به صورت تعاملی استفاده کرد.

این آسیب‌پذیری که با شناسه‌ی CVE-۲۰۱۹-۱۵۹۹۲ معرفی شده است، بر روی تمامی نسخه‌های نرم‌افزاری Cisco ASA و Cisco FTD اثر می‌گذارد.

برای اطلاعات بیشتر و مطالعه تحلیل فنی و
اخبار روز بدافزارها می‌توانید به وب‌سایت‌های
تخصصی امن‌پرداز مراجعه کنید.

WWW.PADVISH.COM