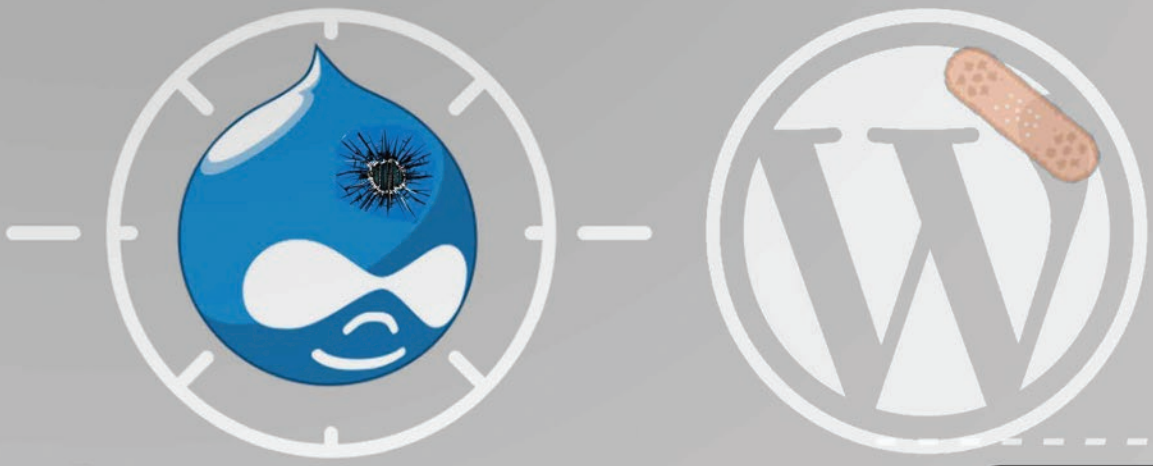
بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و ششم

آبان‌ماه ۱۳۹۹

سیستم‌های مدیریت محتوا در کانون توجه هکرها!



در این شماره می‌خوانید :

اسکیمر جدیدی که از WebSockets برای عدم شناسایی خود استفاده می‌کند

هکرها در جست و جوی میلیون‌ها سیستم مدیریت محتوای وردپرس

آسیب‌پذیری اجرای کد از راه دور در سیستم مدیریت محتوای دروپال

رفع آسیب‌پذیری‌های بحرانی در Cisco Security Manager

دو آسیب‌پذیری روز صفر گوگل کروم

آسیب‌پذیری XSS در Adobe Connect

انتشار باج‌افزار Ryuk در پی آسیب‌پذیری Zerologon

فهرست

- اسکیمر جدیدی که از WebSockets برای عدم شناسایی خود استفاده می‌کند — ۳ اخبار امنیتی
- هکرها در جست و جوی میلیون‌ها سیستم مدیریت محتوای وردپرس — ۴ اخبار امنیتی
- انتشار باج‌افزار Ryuk در پی آسیب‌پذیری Zerologon — ۴ اخبار امنیتی
- رفع آسیب‌پذیری‌های بحرانی در Cisco Security Manager — ۶ آسیب پذیری
- آسیب‌پذیری اجرای کد از راه دور در سیستم مدیریت محتوای دروپال — ۷ آسیب پذیری
- حمله XSS در Adobe Connect — ۷ آسیب پذیری
- دو آسیب‌پذیری روز صفر گوگل کروم — ۸ آسیب پذیری
- 10 نکته برای امن‌سازی ویندوز در سازمان‌ها (بخش دوم) — ۱۰ مقالات آموزشی
- برگزاری سومین دوره مسابقات فتح پرچم در دانشگاه رازی — ۱۲ اخبار داخلی

صاحب امتیاز:
مرکز تخصصی آپا دانشگاه رازی

صفحه آرایی: **سهیلا مرادی، سید احسان حسینی**

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

آدرس:
کرمانشاه، باغ ابریشم، دانشگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

۰۸۳۳۴۳۴۳۲۵۱
apa@razi.ac.ir
@APARazi
cert.razi.ac.ir

اخبار امنیتی

اسکیمر جدیدی که از WebSockets برای عدم شناسایی خود استفاده می‌کند

محققـــان حمله‌ی اســـکیمری جدیـــدی را شناســـایی کرده‌اند که فروشـــگاه‌های اینترنتـــی را با اســـتفاده از یک تکنیک جدید، برای افشـــاء اطلاعـــات کارت‌های بانکی هدف قرار داده است.

عاملان تهدیـــد از فروم‌های[1] جعلیِ کارتِ اعتباری و پروتـــکل WebSockets برای ســـرقت اطلاعات مالی و شـــخص افراد اســـتفاده می‌کنند. امروزه فروشـــگاه‌های اینترنتی با ســـرعت فزاینده‌ای در حال گســـترش هســـتند و اکثراً عملیات پرداخت خـــود را بـــه ارائه‌کنندگان خدمـــات پرداخت شـــخص ثالث واگـــذار می‌کنند و این بدان معناســـت که داده‌هـــای کارت اعتباری را در داخل فروشـــگاه خـــود اداره نمی کننـــد. بنابراین مهاجـــم یک فـــرم کارت اعتباری جعلـــی ایجاد نمـــوده و آن را به صفحه‌ی پرداخـــت برنامه تزریـــق می‌کند و پس از آن، افشـــاء اطلاعـــات خود به خـــود توســـط WebSockets صـــورت می‌گیـــرد. در واقـــع این پروتکل راه را برای مهاجم بسی هموار می‌کند.

در واقع هکرهـــا از اســـکیمرِ نرم‌افزاری به عنـــوان یک اســـکریپت داخلی و برای تزریـــق Loader به کد منبع صفحه اســـتفاده می‌کنند، که به محـــض اجرا یک فایل مخرب جاوااســـکریپت از ســـرور C2 (در آدرس https[:]//tags-manager[.]com/gtags/script2) درخواســـت می‌شـــود. با بارگیری اســـکریپت از ســـرور خارجی، اســـکیمر در LocalStorage مرورگـــر، session-id و آدرس IP کلاینت را ذخیره می‌کند.

مهاجمان با اســـتفاده از Cloudflare's API آدرس IP کاربر را به دســـت می‌آورند، سپس با اســـتفاده از ارتباط WebSocket اطلاعات حساس را از صفحات مربوط به پرداخت، ورود به سیستم و صفحات ثبت‌نام جدید افشاء می‌کنند.

جنبه‌ی متمایزکننـــده‌ی این حمله، اســـتفاده از WebSockets بـــه جای تگ‌های HTML یا درخواســـت‌های XHR برای اســـتخراج اطلاعات از سایت تسخیر شده اســـت که موجب پنهـــان ماندن هر چه بیشـــتر ایـــن تکنیک می‌شـــود. دلیل این

[1] Forum

امر آن است که استفاده از پروتکل WebSocket امکان دور زدن بسیاری از سیاست‌های CSP را فراهم می‌کند.

کارشناسان همچنین مشاهده کردند که در آن دسته از فروشگاه‌های اینترنتی که از ارائه کنندگان خدمات پرداخت شخص ثالث برای عملیات پرداخت خود استفاده می‌کنند، اسکیمر پیش از آنکه صفحه به سمت ارائه‌دهنده‌ی خدمات پرداخت هدایت شود فرم کارت اعتباری جعلی را در صفحه ایجاد می‌کند.

✔ توصیه امنیتی

جهت محافظت از وب‌سایت‌ها در مقابل اسکیمرها، محصول Page Integrity Manager پیشنهاد می‌گردد، که بر اجرا و رفتار اسکریپت‌ها در محیط اجرا تمرکز دارد. این محصول درباره‌ی اسکریپت‌های مختلفی که در صفحه‌ی وب اجرا می‌شوند، هر عملی که انجام می‌دهند و ارتباط آن‌ها با سایر اسکریپت‌های موجود در صفحه اطلاعات جمع آوری می‌کند. انطباق این داده‌ها با رویکرد شناسایی چندلایه_شامل تعیین میزان ریسک، به کارگیری هوش مصنوعی و فاکتورهای دیگر_ به Page Integrity Manager اجازه می‌دهد انواع حملات client-side را با تمرکز بالا بر افشاء اطلاعات و حملات web skimming شناسایی کند.

منبع خبر :

Scan Link

هکرها در جست و جوی میلیون‌ها سیستم مدیریت محتوای وردپرس

نفوذگران ناشناس در حال بررسی فضای وب، جهت شناسایی وب‌سایت‌هایی با سیستم مدیریت محتوای وردپرس هستند که در پوسته‌ی(Theme) آن‌ها از Epsilon Framework استفاده شده است. این پوسته‌ها که در بیش از ۱۵۰،۰۰۰ سایت نصب شده‌اند و در معرض حملات Function Injection قرار دارد که اکسپلویت آسیب‌پذیری های این پوسته‌های وردپرس منجر به تسلط کامل نفوذگر به سایت می‌شود. تاکنون بیش از ۷.۵ میلیون مورد حمله با هدف اکسپلویت آسیب‌پذیری این پوسته‌های وردپرس، از بیش از ۱۸۰۰۰ آدرس IP مختلف، به حدود ۱.۵ میلیون وبسایت وردپرسی، صورت گرفته است.

نسخه‌های ذیل از پوسته‌های وردپرسی آسیب‌پذیر هستند.

- Shapely <=۱.۲.۷
- NewsMag <=۲.۴.۱
- Activello <=۱.۴.۰
- Illdy <=۲.۱.۴
- Allegiant <=۱.۲.۲
- Newspaper X <=۱.۳.۱
- Pixova Lite <=۲.۰.۵
- Brilliance <=۱.۲.۷
- MedZone Lite <=۱.۲.۴
- Regina Lite <=۲.۰.۴
- Transcend <=۱.۱.۸
- Affluent <۱.۱.۰
- Bonkers <=۱.۰.۴
- Antreas <=۱.۰.۲
- NatureMag Lite <=۱.۰.۵

حمله گسترده در حال وقوع علیه سایت‌های وردپرسی، آسیب‌پذیری‌های که اخیرا وصله شدند را هدف قرار داده است. با وجود اینکه آسیب‌پذیری‌ها از نوع اجرای کد از راه دور هستند و مهاجم می تواند اختیار کل سیستم را در دست بگیرد، تاکنون بیشتر حملات با هدف شناسایی سایت دارای پوسته آسیب‌پذیر صورت گرفته‌اند و هدف مهاجمان اکسپلویت آسیب‌پذیری نبوده است.

درصورتی که در وب‌سایت از یکی از این پوسته‌های آسیب‌پذیر استفاده شده باشد، باید هر چه سریع‌تر پوسته آسیب‌پذیر در وب‌سایت به‌روزرسانی شود. همچنین اگر وصله‌ای برای پوسته آسیب‌پذیر وجود نداشته باشد، باید پوسته وردپرس تغییر یابد.

منبع خبر :

Scan Link

انتشار باج‌افزار Ryuk در پی آسیب‌پذیری Zerologon

باج‌افزار Ryuk با هدف قرار دادن سازمان‌های بزرگ در سراسر جهان شناخته شده است. این باج‌افزار اغلب بوسیله بدافزارهای شناخته شده‌ای مانند Emotet و TrickBot

توزیع و منتشر می‌شود.

این باج‌افزار اولین بار در آگوست سال ۲۰۱۸ کشف شد و از آن زمان به بعد سازمان‌های مختلفی را آلوده و میلیون‌ها دلار از قربانیان سرقت کرده است.

تجزیه و تحلیل‌ها نشان می‌دهد که Ryuk نتیجه توسعه سفارشی یک بدافزار قدیمی به نام Hermes است.

اخیراً محققان از ارتباط Ryuk با آسیب‌پذیری خطرناک Zerologon پرده برداشتند.

Zerologon یک آسیب‌پذیری خطرناک است که با شناسه "CVE-2020-1472" شناخته می‌شود، این آسیب‌پذیری به دلیل نقص در فرآیند ورود به سیستم است که به مهاجم اجازه می‌دهد با استفاده از پروتکل Netlogon یا Netlogon Remote Protocol (MS-NRPC)، اتصال یک کانال آسیب‌پذیر Netlogon را با یک کنترل‌کننده دامنه برقرار کند.

بر اساس گزارش DFIR، مهاجمان از طریق بدافزار Bazar Loader به محیط دسترسی نفوذ می‌کنند. در این حمله جدید، مهاجمان سریع‌تر و در مدت زمان ۵ ساعت به هدف خود می‌رسند اما تاکتیک‌ها و تکنیک‌های کلی با حملات قبلی مشابه است.

در این باج‌افزار، مهاجمان به عنوان یک کاربر عادی با دسترسی محدود شروع به کار کرده و با بهره‌برداری از آسیب‌پذیری Zerologon به کنترل‌کننده دامنه اصلی دسترسی پیدا می‌کنند.

اقدامات جانبی به کار گرفته شده از طریق انتقال فایل SMB و اجرای WMI انجام می‌شوند و هنگامی که به کنترل‌کننده دامنه ثانویه منتقل می‌شوند، عاملان تهدید دامنه بیشتری را از طریق Net و ماژول PowerShell Active Directory شناسایی می‌کنند. مهاجمان در حدود ۵ ساعت با اجرای باج‌افزار بر روی کنترل‌کننده دامنه اصلی، هدف خود را به پایان می‌رسانند.

✔ توصیه امنیتی

اولین کاری که باید در سازمان خود انجام دهید این است که اطمینان حاصل کنید که وصله منتشر شده مایکروسافت در شبکه شما اعمال شده است، در صورتی که این عمل صورت نگرفته است بلافاصله نسبت به آن اقدام کنید.

منبع خبر :

Scan Link

اخبار کوتاه

کشف بدافزاری که اطلاعات ۱۵۳ اپ اندرویدی را سرقت می‌کند

اخیراً کارشناسان امنیت سایبری موفق به کشف یک بدافزار اندرویدی به نام «Ghimob» شده‌اند که امکان جاسوسی از کاربران و سرقت اطلاعات را فراهم می‌کند. طبق جدیدترین گزارش کسپرسکی، به نظر می‌رسد این بدافزار اندرویدی توسط گروهی که بدافزار «Astaroth» یا «Guildma» را توسعه داده، به تولید رسیده است.

به گفته این شرکت امنیت سایبری، این تروجان جدید اندرویدی به وسیله اپ‌های مخرب روی دستگاه‌ها نصب می‌شود و درون سایت‌ها و سرورهایی قرار گرفته که در گذشته برای عملیات Astaroth مورد استفاده بوده است.

توزیع این برنامه‌ها توسط فروشگاه رسمی پلی استور صورت نگرفته و بجای این کار، گروه Ghimob از ایمیل‌ها یا سایت‌های مخرب برای هدایت کاربران به سایت‌هایی که این اپ‌های اندرویدی را تبلیغ می‌کردند، هدایت کرده است. این اپ‌ها از برنامه‌های رسمی و برندها تقلید می‌کنند که در میان آن‌ها نام‌هایی مانند گوگل دیفندر، گوگل داکس یا بروزرسانی فلش به چشم می‌خورد.

اگر کاربری بدون توجه به تمام هشدارهای دستگاه خود تصمیم به نصب این برنامه‌ها بگیرد، این اپ‌ها به عنوان آخرین مرحله آلودگی دستگاه، درخواست دسترسی به سرویس «دسترسی‌پذیری» را ارائه می‌کنند. اگر چنین اجازه‌ای به آن‌ها داده شود، این اپ‌ها گوشی کاربر را برای یک لیست حاوی ۱۵۳ برنامه مورد جستجو قرار می‌دهند. این بدافزار در این اپلیکیشن‌ها صفحه ورود جعلی را به نمایش می‌گذارد تا مدارک کاربران را سرقت کند.

پس از یک حمله موفق، اطلاعات و اعتبارنامه‌های کاربران برای گروه Ghimob ارسال می‌شود تا اعضای آن بتوانند به صورت کامل روی دستگاه کنترل داشته باشند و نسبت به هرگونه مشکل امنیتی واکنش نشان دهند. ویژگی‌های این بدافزار منحصر به فرد نیستند و برخی از آن‌ها را در گذشته در تروجان‌های «BlackRock» و «Alien» مشاهده کرده‌ایم.

گوگل از کشف آسیب‌پذیری روز صفر وصله نشده در ویندوز خبر داد

به گفته‌ی گوگل، هکرها از این آسیب‌پذیری روز صفر با نام CVE-2020-17087 و آسیب‌پذیری روز صفر دیگری در کروم (CVE-2020-15999) برای انجام حمله دو مرحله ای استفاده کرده‌اند.

در این گزارش آمده که هکرها با استفاده از آسیب‌پذیری روز صفر کروم کدهای مخرب را درون این مرورگر اجرا کرده و از آسیب‌پذیری ویندوز نیز در قسمت دوم حمله برای فرار از کانتینر امن کروم و اجرای کد در لایه‌های زیرین سیستم‌عامل ویندوز استفاده کرده‌اند.

تیم Zero Project گوگل، مایکروسافت را در جریان این آسیب‌پذیری قرار داده و به آن هفت روز برای برطرف کردن باگ فرصت داده است. این غول نرم‌افزاری در بازه هفت روزه موفق به عرضه وصله‌ی امنیتی نشد، به همین دلیل گوگل جزئیات این آسیب‌پذیری را به شکل عمومی منتشر کرده است.

تیم امنیتی گوگل جزئیات گروه‌های هکی که در حال سوء استفاده از این آسیب‌پذیری هستند را فاش نکرد، اما اکثر آسیب‌پذیری‌های روز صفر معمولاً توسط هکرهای وابسته به دولت‌ها یا گروه‌های جرایم سایبری بزرگ مورد سوءاستفاده قرار می‌گیرند. لازم به ذکر است که آسیب‌پذیری روز صفر کروم در نسخه ۸۶.۰.۴۲۴۰.۱۱۱ این مرورگر رفع شده است.

آسیب پذیری

رفع آسیب‌پذیری‌های بحرانی در Cisco Security Manager

یک نقص بحرانی path-traversal با شناسه CVE-2020-27130 در Cisco Security Manager وجود دارد که اطلاعات حساس زیادی را در اختیار مهاجم از راه دور قرار می‌دهد. Cisco Security Manager یک برنامه مدیریت امنیت برای مدیران سازمانی است که به آن‌ها امکان اجرای انواع سیاست‌های امنیتی، عیب‌یابی رخدادهای امنیتی و مدیریت طیف وسیعی از دستگاه‌ها را می‌دهد.

آسیب‌پذیری مذکور دارای شدت بحرانی و امتیاز ۹.۱ از ۱۰ در سیستم امتیازدهی CVSS می‌باشد. به گفته‌ی سیسکو، "مهاجم با ارسال یک درخواست جعلی و ساختگی به دستگاه آسیب‌پذیر می‌تواند از این آسیب‌پذیری بهره‌برداری نماید." بهره‌برداری موفق از این آسیب‌پذیری امکان دانلود فایل‌های دلخواه را از دستگاه آسیب‌پذیر برای مهاجم فراهم می‌آورد. علت این آسیب‌پذیری اعتبارسنجی نامناسب توالی‌های کاراکتر directory traversal در درخواست‌های ارسالی به یک دستگاه آسیب‌پذیر است. حمله‌ی path-traversal با هدف دسترسی به فایل‌ها و دایرکتوری‌هایی است که خارج از پوشه‌ی root ذخیره شده‌اند. اگر مهاجم متغیرهای مربوط به ارجاع فایل‌ها را دستکاری کند (با توالی‌های دات دات اسلش (/..))، امکان دسترسی به فایل‌ها و دایرکتوری‌های ذخیره شده در فایل سیستم، مانند کد منبع برنامه یا فایل‌های سیستمی مهم و فایل پیکربندی را خواهد داشت.

سیسکو همچنین دو آسیب‌پذیری دیگر با شدت بالا را در برنامه Cisco Security Manager برطرف نموده است. یکی از این آسیب‌پذیری‌ها با شناسه‌ی CVE-2020-27125 دارای شدت بالا و امتیاز ۷.۴، ناشی از حفاظت ناکافی از اطلاعات ورود استاتیک در نرم‌افزار آسیب‌پذیر است. این آسیب‌پذیری به مهاجم از راه دور و احراز هویت نشده اجازه می‌دهد به اطلاعات حساس در سیستم آسیب‌پذیر دسترسی پیدا کند.

به گفته‌ی سیسکو، "مهاجم با مشاهده‌ی کد منبع برنامه می‌تواند از این آسیب‌پذیری بهره‌برداری نماید." بهره‌برداری موفق از این آسیب‌پذیری به مهاجم امکان مشاهده‌ی اطلاعات ورود استاتیک را می‌دهد که می‌تواند در حملات بعدی از آن‌ها استفاده کند.

آسیب‌پذیری دوم با شناسه‌ی CVE-2020-27131 دارای شدت بالا و امتیاز ۸.۱، در تابع deserialization جاوا وجود دارد که توسط Cisco Security Manager مورد استفاده قرار می‌گیرد و به مهاجم احراز هویت نشده‌ی از راه دور اجازه می‌دهد تا دستورات دلخواه خود را در دستگاه آسیب‌پذیر اجرا نماید. این آسیب‌پذیری ناشی از محتوای ناامن ارائه شده توسط کاربر در تابع deserialization است.

مهاجم با ارسال یک شیء مخرب serialized جاوا به یک شنونده‌ی خاص در دستگاه آسیب‌پذیر می‌تواند از این آسیب‌پذیری بهره‌برداری نماید. بهره‌برداری موفق از این آسیب‌پذیری به مهاجم اجازه می‌دهد دستورات دلخواه خود را بر روی دستگاه با دسترسی NT AUTHORITY\SYSTEM در میزبان هدف ویندوزی اجرا نماید.

نسخه‌های تحت تأثیر آسیب‌پذیری

آسیب‌پذیری‌های CVE-2020-27130 و CVE-2020-27125 نسخه‌ی ۴.۲۱ برنامه و نسخه‌های ماقبل آن، و آسیب‌پذیری CVE-2020-27131 نسخه‌ی ۴.۲۲ برنامه و نسخه‌های ماقبل آن را تحت تأثیر قرار می‌دهد.

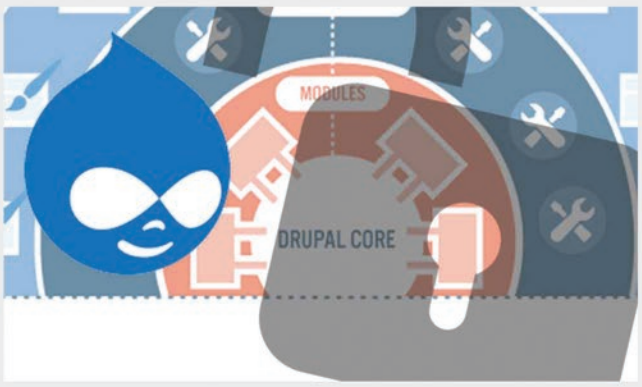
راهکار

آسیب‌پذیری‌های CVE-2020-27130 و CVE-2020-27125 در نسخه‌ی ۴.۲۲ و آسیب‌پذیری CVE-2020-27131 در نسخه‌ی ۴.۲۳ از برنامه‌ی Cisco Security Manager برطرف شده‌اند.

منبع خبر :

Scan Link

آسیب‌پذیری اجرای کد از راه دور در سیستم مدیریت محتوای دروپال



تیم توسعه دروپال به‌روزرسانی امنیتی را برای رفع آسیب‌پذیری اجرای کد از راه دور منتشر کرده است. این آسیب‌پذیری ناشی از عدم فیلتر (sanitize) دقیق نام فایل‌های آپلودی می‌باشد. این آسیب‌پذیری که با شناسه CVE-2020-13671 پیگیری می‌شود، بر اساس سیستم امتیاز دهی استاندارد NIST Common Misuse Scoring System در دسته‌بندی شدت اهمیت بحرانی قرار دارد. برای رفع این آسیب‌پذیری کافیست آخرین نسخه دروپال نصب شود.

- اگر از نسخه‌های سری ۹.۰ از دروپال استفاده می‌کنید، سیستم مدیریت محتوای خود را به نسخه ۹.۸.۰ از دروپال به‌روزرسانی کنید.
- اگر از نسخه‌های سری ۸.۹ از دروپال استفاده می‌کنید، سیستم مدیریت محتوای خود را به نسخه ۸.۹.۹ از دروپال به‌روزرسانی کنید.
- اگر از نسخه ۸.۸ از دروپال یا نسخه‌های قبل‌تر از این نسخه استفاده می‌کنید، سیستم مدیریت محتوای خود را به نسخه ۸.۸.۱۱ از دروپال به‌روزرسانی کنید.
- اگر از نسخه‌های سری ۷ از دروپال استفاده می‌کنید، سیستم مدیریت محتوای خود را به نسخه ۷.۷۴ به‌روزرسانی کنید.

نسخه‌های سری ۸ از دروپال که پیش از انتشار نسخه‌های ۸.۸.x منتشرشده‌اند، منسوخ شده هستند و تیم دروپال امنیت این نسخه‌ها از دروپال را پشتیبانی نمی‌کند. تیم دروپال همچنین توصیه کرده است تا تمام فایل‌هایی که پیش از به‌روزرسانی در سامانه آپلود شده‌اند با هدف شناسایی پسوندهای مخرب بررسی شوند. به ویژه در جست‌وجوی فایل‌هایی با دو پسوند مانند filename.php.txt یا filename.html.gif باشید که شامل (_) در پسوند نباشند. در مواردی که فایل‌های آپلود شده دارای یک یا چند پسوند از پسوندهای ذکر شده در ذیل باشد؛ لازم است، این فایل با دقت بیشتری بررسی شود.

- Phar
- phtml
- php
- pl
- py
- cgi
- asp
- js
- html
- htm

توجه کنید این لیست جامع نیست، بنابراین هر پسوند غیر مجازی با دقت بررسی شود.

منبع خبر :

Scan Link

آسیب‌پذیری XSS در Adobe Connect

محققان حوزه امنیت اخیراً از مشاهده یک آسیب‌پذیری با شناسه CVE-2020-24442 و شدت ۳.۵ از ۱۰ (شدت پایین) در سیستم امتیازدهی CVSS در Adobe Connect خبر داده‌اند که بر روی برخی از قابلیت‌هاي این سیستم که امروزه کاربران زیادی دارد، تأثیرمی‌گذارد. طبق گفته محققین، ایجاد تغییرات در سیستم به همراه ورودی ناشناخته، منجر به آسیب‌پذیری XSS می‌شود. لذا ممکن است یک مهاجم بتواند کد HTML و اسکریپت دلخواه را به وب‌سایت تزریق کند. این امر باعث تغییر ظاهر و شروع حملات بیشتر علیه بازدیدکنندگان سایت می‌شود.

به گفته محققین، بهره‌برداری از این آسیب‌پذیری بسیار آسان است، به نحوی که می‌توان گفت شروع حمله از راه دور نیز امکان‌پذیر است. اما احراز هویت برای بهره‌برداری از این آسیب‌پذیری مورد نیاز می‌باشد. در واقع این آسیب‌پذیری، به یک مهاجم از راه دور اجازه می‌دهد تا حملات XSS را انجام دهد.

این آسیب‌پذیری به دلیل پاک نکردن صحیح اطلاعات ارائه شده توسط کاربر به وجود آمده است. یک مهاجم از راه دور می‌تواند قربانی را فریب دهد تا یک پیوند خاص ساخته شده را دنبال کند و کد HTML و اسکریپت دلخواه را در مرورگر کاربر اجرا کند. یک سوءاستفاده موفقیت‌آمیز از این آسیب‌پذیری ممکن است به مهاجم امکان سرقت اطلاعات حساس، تغییر شکل صفحه وب و انجام حملات فیشینگ را بدهد.

نسخه‌های تحت تأثیر آسیب‌پذیری

این آسیب‌پذیری، تمام نسخه‌های زیر از Adobe Connect را تحت تاثیر قرار می‌دهد:

۹.۰, ۹.۰.۱, ۹.۰.۲, ۹.۰.۳, ۹.۰.۴, ۹.۱, ۹.۱.۱, ۹.۱.۲, ۹.۲, ۹.۲.۱, ۹.۲.۲, ۹.۳, ۹.۴, ۹.۴.۱, ۹.۴.۲, ۹.۵, ۹.۵.۱, ۹.۵.۲, ۹.۵.۳, ۹.۵.۴, ۹.۵.۵, ۹.۵.۶, ۹.۵.۷, ۹.۶.۱, ۹.۶.۲, ۹.۷, ۹.۷.۵, ۹.۸, ۹.۸.۱, ۱۰.۰, ۱۰.۰.۱, ۱۱.۰.

راهکار

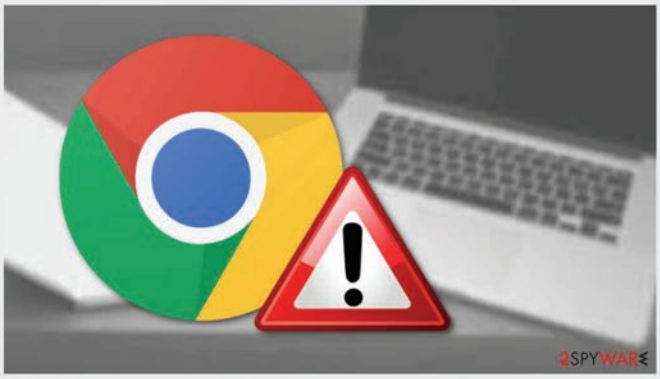
برای رفع این آسیب‌پذیری شرکت Adobe نسخه جدیدی از Adobe Connect را منتشر کرده است. به‌روزرسانی به نسخه ۱۱.۰.۵ سبب رفع این آسیب‌پذیری می‌شود که این نسخه برای بارگیری در helpx.adobe.com میزبانی می‌شود. در ادامه لینک صفحه دانلود قرار داده شده است:

https://helpx.adobe.com/adobe-connect/connect-downloads-updates.html

منبع خبر :

Scan Link

دو آسیب‌پذیری روز صفر گوگل کروم



گوگل نسخه ۸۶.۰.۴۲۴۰.۱۹۸ از گوگل کروم را برای ویندوز، لینوکس و Mac به منظور رفع دو آسیب‌پذیری روز صفر که به صورت عمومی در حال اکسپلویت است، منتشر کرده است. جهت به‌روزرسانی گوگل کروم به صورت خودکار، لازم است امکان به‌روزرسانی خودکار در این مرورگر از مسیر 'About -> Help -> Settings Google Chrome' فعال شود.

هر دو آسیب‌پذیری روز صفر توسط محققان ناشناس به گوگل گزارش شده است، اما این شرکت هیچگونه توضیحی در مورد حملاتی که از این آسیب‌پذیری‌ها استفاده می‌کند و نفوذگران پشت این حملات نداده است. یکی از این آسیب‌پذیری‌ها که با شناسه CVE-2020-16013 شناخته می‌شود، مرتبط با پیاده‌سازی نادرست موتور منبع باز WebAssembly وJavaScript گوگل کروم است. دومین آسیب‌پذیری که با شناسه CVE-2020-16017 شناخته می‌شود، مرتبط با استفاده از حافظه آزاد شده در پروژه Site Isolation گوگل است که منجربه اجرای کد دلخواه از راه دور می‌شود.

گوگل بیان کرده است تا زمانی‌که اکثریت کاربران مرورگر خود را به‌روزرسانی نکرده باشند؛ جزئیات این باگ‌ها منتشر نخواهد شد. کاربران گوگل کروم بایستی توجه نمایند، در طی یک ماه گذشته، ۵ آسیب‌پذیری روزصفر در مرورگر گوگل کروم به‌روزرسانی شده است. لذا توصیه می‌شود قابلیت به‌روزرسانی خودکار در این مرورگر را فعال نمایید.

منبع خبر :

Scan Link

اخبار کوتاه

فایرفاکس ۸۳ با سرعت و امنیت بالاتر منتشر شد

موزیلا از انتشار آخرین نسخه «فایرفاکس ۸۳» برای کاربران سیستم‌عامل‌های ویندوز، مک و لینوکس خبر داد. یکی از ویژگی‌های برجسته امنیتی این نسخه حالت «HTTPS-Only» است. سرعت عملکرد نسخه جدید نیز نسبت به نسخه قبل بهبود یافته است.

براساس اعلام موزیلا، فایرفاکس حدود ۲۲۵ میلیون کاربر فعال دارد و همین موضوع، آن را به بستری اصلی برای توسعه‌دهندگان وب تبدیل کرده است.

با کمک ویژگی جدید امنیتی «HTTPS-Only Mode»، تمامی وب‌سایت‌ها از طریق HTTPS بارگذاری می‌شوند. در واقع ویژگی جدید سعی می‌کند نسخه HTTPS سایت را بارگذاری کند. اگر نتواند نسخه مربوطه را بارگذاری کند؛ برای اتصال به وب‌سایت از کاربر سوال می‌کند و هشدار می‌دهد که در حال اتصال به وب‌سایتی با پروتکل قدیمی و ناامن HTTP است.

این ویژگی جدید به صورت پیش‌فرض، غیرفعال است. کاربران می‌توانند با مراجعه به قسمت Firefox Options و سپس مراجعه به بخش Privacy & Security، تنظیمات حالت HTTPS-Only را فعال کنند.

فایرفاکس ۸۳ کماکان از فلش‌پلیر پشتیبانی می‌کند؛ اما زمانی که فایرفاکس ۸۵ در تاریخ ۲۳ دی‌ماه از راه برسد، ادوب‌فلش‌پلیر کاملا غیر فعال خواهد شد.

آسیب‌پذیری جدید اندروید ۹

محققان امنیتی تقریباً در هر نسخه Android آسیب‌پذیری بزرگی را یافته‌اند که به بدافزارها اجازه می‌دهد تا از برنامه‌های قانونی برای سرقت رمزهای عبور برنامه و سایر داده‌های حساس تقلید کنند.

این آسیب‌پذیری موسوم به StrandHogg ۲.۰ بر تمام دستگاه‌های دارای اندروید نسخه ۹.۰ و پیش از آن تأثیر می‌گذارد.

نسخه قبلی این باگ، StrandHogg ۱.۰ که در حدود شش ماه قبل کشف شده است به همراه نسخه جدید آن (StrandHogg ۲.۰) به نام "دوقلو شر"(evil twin) نامیده می‌شوند. StrandHogg ۲.۰ با فریب دادن یک قربانی گذرواژه‌های خود را در یک برنامه قانونی وارد می‌کند و در عوض با یک پوشش مخرب ارتباط برقرار می‌کند.

StrandHogg ۲.۰ همچنین می‌تواند مجوزهای برنامه دیگر را برای فریب داده‌های حساس کاربر مانند مخاطبین، عکس‌ها و ردیابی مکان واقعی مورد سرقت قرار دهد.

این بدافزار می‌تواند مکالمات پیام متنی را بارگذاری کند، و به هکرها اجازه می‌دهد محافظت در تأیید هویت دو عاملی را شکست دهند. خطر برای کاربران احتمالاً کم است، اما صفر نیست.

به روزرسانی دستگاه‌های Android با جدیدترین نسخه‌های امنیتی می‌تواند این آسیب‌پذیری را برطرف کند.

به کاربران توصیه می‌شود در اسرع وقت دستگاه‌های اندرویدی خود را به روز کنند.

محققان برای اولین بار توانستند کلید رمزنگاری کدهای پردازنده‌های اینتل را به دست آورند

محققان اخیراً توانسته‌اند کلید رمزنگاری به‌روزرسانی‌ها را در برخی از پردازنده‌های شرکت اینتل به دست آورند. این دستاورد می‌تواند پیامدهایی گسترده به همراه داشته باشد و احتمالاً چگونگی استفاده از چیپ‌ها و همین‌طور چگونگی امن‌سازی آن‌ها را دست‌خوش تغییرات اساسی کند.

این کلید به پردازنده‌ها اجازه می‌دهد که قادر به رمزگشایی به‌روزرسانی‌های مایکروکدی باشند که اینتل برای برطرف‌سازی آسیب‌پذیری‌های امنیتی و دیگر باگ‌ها منتشر می‌کند.

با دسترسی داشتن به یک کپی رمزگشایی شده از آپدیت‌ها، هکرها می‌توانند کدنویسی‌ها را مهندسی معکوس کنند و دقیقاً بیاموزند که فلان حفره امنیتی چطور برطرف شده است.

این کلید ضمنا به اشخاص ثالث اجازه می‌دهد که چیپ‌ها را با مایکروکد مخصوص خود آپدیت کنند، هرچند که این نسخه شخصی‌سازی شده بعد از ریبوت از دست می‌رود.

علی‌رغم تمام این موضوعات، محققان می‌گویند که در نهایت یک پیامد بسیار مهم خواهیم داشت: تحلیل مستقل مایکروکدهای اینتل که تا به امروز غیرممکن بوده است.

حالا باید دید که اینتل چطور در صدد برطرف‌سازی این مشکل برمی‌آید.

رفع سه آسیب‌پذیری روز صفر در iOS توسط Apple

Apple با انتشار نسخه ۱۴.۲ از iOS سه آسیب‌پذیری روز صفر با شناسه‌های CVE-2020-27932، CVE-2020-27930 و CVE-2020-27950 در iOS را که به صورت فعال اکسپلویت می‌شوند رفع کرده است. توصیه می‌شود کاربران iOS برای رفع این سه آسیب‌پذیری هرچه سریع‌تر نسخه ۱۴.۲ از iOS را نصب نمایند.

این آسیب‌پذیری‌های محصولات زیر را تحت تاثیر قرار می‌دهد.

- iPhone ۶ و نسخه‌های بعد از آن
- touch iPod نسل ۷
- iPad Air ۲ و نسخه‌های بعد از آن
- iPad mini ۴ و نسخه‌های بعد از آن

این آسیب‌پذیری‌ها با سه آسیب‌پذیری اخیر گوگل با شناسه‌های CVE-2020-17087 CVE-2020-16009 و CVE-2020-16010 و آسیب‌پذیری سیستم‌عامل ویندوز با شناسه CVE-2020-17087 مرتبط است.

کارشناسان خاطر نشان کرده‌اند که سوءاستفاده از این سه نقص به صورت زنجیره‌ای موجب می‌شود تا هکرها بتوانند از راه دور دستگاه‌های iPhone را به صورت کامل در اختیار بگیرند.

هکرها به ساخت نسخه‌های لینوکس باج‌افزارها روی آورده‌اند!

شرکت کسپرسکی از کشف نسخه لینوکس باج افزار RansomEXX خبر داد. این یعنی برای اولین بار نسخه لینوکس یک باج افزار خطرناک ویندوزی برای بکارگیری در حملات هدفمند توسعه داده شده است.

RansomEXX باج افزار نسبتاً جدیدی است که اولین بار ژوئن سال جاری میلادی کشف شد. به گفته کسپرسکی توسعه نسخه لینوکس این باج افزار در راستای مهاجرت بسیاری از شرکت‌ها به لینوکس رخ داده و دیگر مثل گذشته تمام سیستم‌ها با ویندوز سرور اجرا نمی‌شوند. نسخه لینوکس RansomEXX به هکرها این توانایی را می‌دهد تا ابعاد حمله را تا جای ممکن گسترش داده و با آلوده کردن سیستم‌های بیشتر، مبلغ باج را افزایش دهند.

توسعه نسخه لینوکس باج افزارها ترند خواهد شد و احتمالاً در آینده نزدیک شاهد عرضه باج افزارهای خطرناک بیشتری برای این سیستم عامل خواهیم بود.

مقالات آموزشی

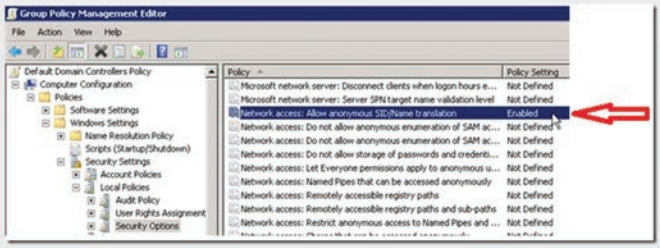
۱۰ نکته برای امن‌سازی ویندوز در سازمان‌ها (بخش دوم)

یکی از راه‌های معمول اعمال قوانین واجازه سطح دسترسی‌های مختلف در کامپیوترهای ویندوزی مایکروسافت در سازمان‌ها، گروپ‌پالیسی‌ها می‌باشد. در اکثر موارد گروپ‌پالیسی‌ها تنظیماتی به منظور پیکربندی تنظیمات امنیتی و دیگر رفتارهای عملیاتی هستند که بر روی رجیستری کامپیوترها می‌نشینند.

گروپ‌پالیسی‌ها می‌توانند توسط اکتیودایرکتوری یا Local group policy پیکربندی و اعمال شوند. این قابلیت تنظیم و پیکربندی تنظیمات امنیتی با استفاده از گروپ‌پالیسی، یکی از بزرگترین مزیت‌های کار کردن با کامپیوترهایی است که سیستم‌عامل‌های آن‌ها ویندوزی است. بخش اول این آموزش در بولتن شماره قبلی منتشر شد. حال در بخش دوم این آموزش، در این شماره از بولتن خبری می‌خواهیم به ۵ نکته بپردازیم که در صورت در نظر گرفتن آن‌ها تا حد قابل قبولی امنیت سازمان شما حفظ می‌شود، اکثر این تنظیمات به پیکربندی Group Policy مربوط می‌شوند.

۱. غیر فعال کردن Anonymous SID

SIDها (شناسه امنیت) شناسه‌هایی هستند که به هر کاربر، گروه و دیگر اشیاء امنیتی در ویندوز یا اکتیودایرکتوری اختصاص داده شده‌اند. در نسخه‌های قبلی سیستم‌عامل، کاربران احراز هویت نشده می‌توانستند این شناسه‌ها را برای تشخیص کاربران مهم به عنوان مثال Administratorها بکار گیرند. درواقع این یکی از مشکلات امنیتی بود که هکرها علاقه زیادی به بهره‌برداری از آن داشتند. به این منظور در Run تایپ کنید Secpol.msc و کلید Enter را بزنید و با توجه به شکل زیر مسیر را ادامه دهید.



شکل ۱: غیرفعال کردن Anonymous SID/Name در ویندوز

پس از یافتن گزینه Network access: Allow anonymous SID/Name translation بر روی آن دابل کلیک نموده و چک‌باکس Disabled را انتخاب کنید.

۲. سیستم باید به گونه‌ای پیکربندی شود که کاربران ناشناخته (Anonymous) حقوق یکسان برای دسترسی به هر گروه را نداشته باشند.

دسترسی‌های کاربران Anonymous باید محدود شوند. اگر این تنظیمات فعال باشند کاربران Anonymous می‌توانند حقوق یکسان و مجوز دسترسی به گروه های سیستمی را داشته باشند.

بدین معنا که هکرهای ناشناخته می‌توانند از راه دور و از طریق همین کاربران اضافی و ناشناس، به سیستم‌های داخل سازمان دسترسی کامل پیدا کنند.بنابراین کاربران anonymous نباید این مجوز و حقوق را داشته باشند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

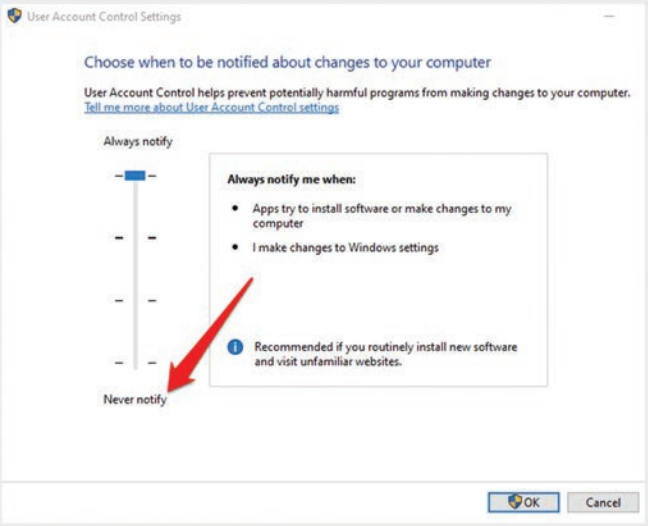
Windows Settings -> Security Settings -> Local Policies -> Security Options ->

"Network access: Let everyone permissions apply to anonymous users" to "Disabled".

۳. فعال کردن User Account Control

از ویندوز ویستا به بعد UAC به یکی از مهم‌ترین ابزارهای حفاظتی برای ویندوز و کاربرانی که دروب جستجو می‌کنند تبدیل شده است. متأسفانه تعداد زیادی از کاربران این ابزار امنیتی را به خاطر به وجود آوردن برخی از مشکلات عدم سازگاری نرم‌افزارها به پایین‌ترین حد امنیتی کاهش می‌دهند که کاملاً اشتباه است. با این کار ممکن است برخی از این مشکلات رفع شود اما امکان قرار گرفتن در معرض آسیب‌هایی وجود دارد که ممکن است سیستم را در معرض خطر قرار دهند. از این رو پیشنهاد می‌شود که این ابزار را غیرفعال نکنید.

برای غیرفعال کردن UAC در ویندوز ۷، ۸ و یا ۱۰ روی دکمه Start کلیک کنید و در کادر جستجو عبارت UAC را تایپ کنید، از لیست نتایج Change User Account Control settings را انتخاب کنید، سپس مطابق شکل زیر آن را فعال‌نمایید.



شکل ۲: فعال سازی User Account Control در ویندوز

۴. تغییر نام کاربری Administrator

حساب کاربری Administrator موجود (سیستمی) یک حساب کاربری شناخته شده برای حمله است. تغییر نام‌دادن حساب کاربری به نام ناشناس حفاظت از این حساب کاربری و سیستم را بهبود می‌بخشد. در واقع، زمانی که نام حساب کاربری Administrator را تغییر می‌دهید برخی از هکرهای مبتدی که دانش زیادی ندارند قادر به هک کردن سیستم شما نیستند که این امر درصد هک شدن را کاهش می‌دهد، البته این نکته را هم باید ذکر کرد که هکرهایی که دانش بالایی دارند می‌توانند کاربرانی را که دسترسی Admin دارند از روی SID آن‌ها تشخیص دهند.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options ->

"Accounts:Rename administrator account" to a name other than "Administrator".

۵. Guest Account را غیرفعال کنید.

اگر این ویژگی غیرفعال نشود سیستم در معرض افزایش تهدید آسیب‌پذیری قرار می‌گیرد. این حساب کاربری یک حساب کاربری شناخته شده است که برروی تمام سیستم‌های ویندوزی وجود دارد و نمی‌توان آن را پاک کرد. به این حساب کاربری در طول نصب و راه‌اندازی اولیه سیستم عامل هیچ کلمه عبوری اختصاص داده نمی‌شود.

نحوه پیاده‌سازی: پیکربندی مقدار این خط مشی طبق مسیر زیر است:

Windows Settings -> Security Settings -> Local Policies -> Security Options ->

"Accounts: Guest account status" to "Disabled".

اخبار کوتاه

برای برطرف کردن آسیب‌پذیری جدی در بازی‌های فروشگاه مایکروسافت، ویندوز ۱۰ خود را به روز کنید.

آسیب‌پذیری که با عنوان CVE-2020-16877 ردیابی شده است و دارای شدت بالا می‌باشد بر ویندوز سرور و ویندوز ۱۰ تأثیر می‌گذارد. پژوهشگران امنیت سایبری IOActive آسیب‌پذیری بالا بردن سطح دسترسی _privilege escalation_ را در سیستم‌های ویندوزی افشا کرده‌اند، که می‌تواند از طریق سوءاستفاده از بازی‌های آپلود شده در فروشگاه مایکروسافت مورد بهره‌برداری قرار گیرد.

محققان یک بازی را با مودهای آن دانلود کردند و فرآیند پردازش را برآورد کردند. آن‌ها شناسایی کردند که یك مهاجم به راحتی می‌تواند با حذف یا بازنویسی مجدد فایل‌های دلخواه روی سیستم با ایجاد سیملینک- symlinks، به راحتی از پردازش سوءاستفاده کرده و سطح دسترسی خود را بالا ببرد.

Ferrante، محققی که این آسیب‌پذیری را گزارش نمود، پیوندهای مشترکی بین پوشه ModifiableWindowsApps و پوشه ذخیره شده در درایو دیگری که می توانست به آن دسترسی داشته باشد، تشکیل داد. مایکروسافت پوشه ModifiableWindowsApps را برای ذخیره‌سازی بازی‌ها ایجاد می‌کند. Ferrante از طریق این روش پردازش نصب را ربوده و از طریق بازنویسی و حذف فایل‌های روی سیستم امتیازات بالایی را کسب کرد.

مایکروسافت این آسیب‌پذیری را با پچ اکتبر (October's Patch Tuesday) خود برطرف کرد. با این حال، مخربین هنوز هم می‌توانند در صورتی که سیستم هدف تا آخرین نسخه به‌روز نشده باشد، از این آسیب‌پذیری برای دستیابی به افزایش سطح دسترسی در سیستم‌های مبتنی بر ویندوز از طریق فروشگاه مایکروسافت استفاده کنند.

سومین دوره مسابقات فتح پرچم دانشگاه رازی

مسابقات فتح پرچم مرکز آپا دانشگاه رازی برای اولین بار در سال ۱۳۹۶ به شکل منطقه‌ای و دومین دوره آن سال گذشته به شکل ملی برگزار شد و امسال با توجه به تجربیات موفق به دست آمده در دو دوره‌ی گذشته، این مسابقات به شکل بین‌المللی برگزار گردید.

با توجه به اولین تجربه‌ی دانشگاه رازی در برگزاری این مسابقات به شکل بین‌المللی، استقبال تیم‌های داخلی و خارجی از آن بسیار خوب و چشمگیر بود.

سومین دوره مسابقات فتح پرچم دانشگاه رازی،که امسال برای نخستین بار در سطح بین‌المللی برگزار گردید، در تاریخ ۵ آبان ماه ۱۳۹۹ آغاز و ۷ آبان ماه، رأس ساعت ۹ صبح به پایان رسید. در این مسابقات ۶۱۳ تیم از ۵۵ کشور در سراسر جهان شرکت کردند که پس از ۴۸ ساعت رقابت تنگاتنگ پرچم‌های خود را فتح نمودند. از این آمار ۱۰۳ تیم ایرانی بودند. رتبه‌بندی تیم‌های برتر این مسابقات به شرح زیر می‌باشند:

تیم‌های برتر سومین دوره مسابقات فتح پرچم دانشگاه رازی			مجموع امتیازات
1	EPT		41992
1	irNoobs		38001
3	bootplug		36997
4	AlphaPwners		36009
2	TMU		32143
3	NaRazi		32030
7	Fword		31043
8	Corax		28136
9	ByteForc3		28064
10	Terminox		27639

شکل ۳: رتبه‌بندی تیم‌های برتر سومین دوره مسابقات فتح پرچم دانشگاه رازی

برای تیم‌های شرکت‌کننده در این مسابقات ۵۵ چالش در ۱۰ حوزه امنیت سایبری طراحی شد که آن‌ها فرصت داشتند طی دو روز با عبور از این چالش‌ها به هدف نهایی که دستیابی به پرچم است، برسند. مهندسی معکوس، رمزنگاری، امنیت وب، امنیت شبکه، جرم‌شناسی، امنیت سیستم‌های کنترل صنعتی، پنهان‌نگاری، جاسوسی محترمانه، تسخیر و امنیت اندروید، ۱۰ حوزه‌ای است که چالش‌ها در قالب آن‌ها طراحی شدند.

همانطور که در شکل ۳ قابل مشاهده است، تیم‌های ایرانی جایگاه خوبی در میان کل تیم‌های شرکت‌کننده دارند و این نشان‌دهنده‌ی مهارت بالای این تیم‌ها در حوزه‌های مختلف امنیت سایبری است. این مسابقات با هدف ترغیب دانشجویان به پژوهش در خصوص موضوعات امنیت سایبری، شناسایی افراد مستعد در بخش امنیت، تربیت افسران نیروی سایبری، جذب نیروی متخصص و افزایش آمادگی و توانمندی علاقه‌مندان برای شرکت در مسابقات بین‌المللی برگزار شده است. با توجه به کسب امتیاز بالای تیم‌های ایرانی در این مسابقه، امید است بتوانیم از توانایی و مهارت این افراد در جهت قوی‌تر نمودن تیم امنیت سایبری ملی استفاده نموده و به جایگاهی که شایسته‌ی آن‌هاست برسانیم.

تیم‌های برتر ایرانی:

تیم اول: irNoobs

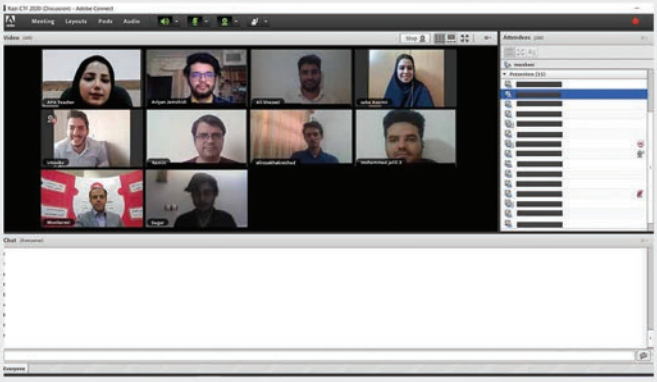
تیم دوم: TMU

تیم سوم: NaRazi

اختتامیه سومین مسابقه فتح پرچم دانشگاه رازی

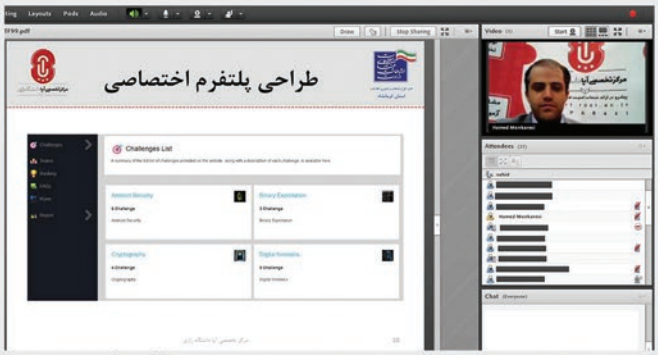
همزمان با روز گرامی‌داشت پدافند غیرعامل، ۸ آبان ماه ۱۳۹۹ ساعت ۱۰ صبح، مراسم اختتامیه سومین دوره مسابقات فتح پرچم در دانشگاه رازی با شرکت مهمانان و برگزیدگان مسابقه به صورت آنلاین برگزار گردید.

در این مراسم ضمن ارائه آمار و اطلاعات تخصصی در خصوص چالش‌های ارائه شده در این مسابقه، برگزیدگان این دوره از مسابقات نیز به ارائه نظرات و پیشنهادات خود پرداختند.



شکل ۴: مراسم اختتامیه سومین دوره مسابقات فتح پرچم دانشگاه رازی

همچنین در این مراسم عنوان شد که پلتفرم بومی این مسابقات که در مرکز آپا دانشگاه رازی تولید شده است، بزودی به صورت عمومی در اختیار علاقه‌مندان قرار خواهد گرفت.



شکل ۵: پلتفرم بومیِ طراحی شده برای مسابقات فتح پرچم، توسط مرکز آپا دانشگاه رازی

وبینار چالش‌های نوین در امنیت شبکه

پیشرفت دنیای شبکه‌های کامپیوتری و توسعه تکنولوژی‌های نوظهوری مانند SDN، cloud و فراهم آمدن ظرفیت‌های جدیدی از اتوماسیون شبکه و قابلیت‌های programability که ارائه سرویس‌های تحت شبکه را متحول و طوفانی در شبکه‌های سنتی به راه انداخته، به تناسب، چالش‌ها و مخاطرات امنیتی مختلفی هم به همراه آورده است. ظرفیتی که اجرای اسکریپت‌های زبان‌های برنامه نویسی در پلتفرم‌های programable جدید که اساس شبکه‌های مدرن امروزی بر آن بنا شده در اختیار قرار می‌دهد، می‌تواند مانند چاقویی دولبه در اختیار هکرها نیز قرار گیرد. متأسفانه سرعت تحول و توسعه این تکنولوژی آنقدر بالا بوده که راهکارهای امنیتی هنوز نتوانسته‌اند بر تهدیدهای آن فائق آیند و این باعث ایجاد یک خلاء خطرناک در حوزه امنیت شده است. البته در همه ساختارها و تکنولوژی‌ها در دوره حالت گذار و عبور از حالت سنتی به حالت نوین که اکنون در دنیای فناوری اطلاعات در حال رخ دادن است این خلأ ایجاد می‌شود. از این رو برای مدیران شبکه و متخصصان امنیت ضروری است که با این تهدیدها آشنا شده و بتوانند چاره‌ای برای آن‌ها بیندیشند. به همین منظور وبینار چالش‌های نوین در امنیت شبکه در مورخ ۲۲ آبان ماه ۱۳۹۹ با شرکت پرسنل بخش خصوصی و دولتی سازمان‌ها، دانشجویان و علاقمندان برگزار شد. در این وبینار شرکت‌کنندگان با چالش‌های این تکنولوژی‌ها آشنا شده و سعی شد راه حلی منطقی برای آن‌ها ارائه شود.

اخبار کوتاه

مراقب دست‌فروشان اسکیمری باشید!

با توجه به اینکه دست‌فروشان می‌توانند محل کسب و کار خود را به راحتی تغییر دهند، کلاهبرداران در قالب دستفروش دوره‌گرد با استفاده از اسکیمر اقدام به سرقت اطلاعات کارت بانکی شهروندان کرده و حساب بانکی آن‌ها را خالی می‌کنند.

اسکیمر دستگاهی است که قابلیت کپی کردن اطلاعات کارت‌های اعتباری بانکی را داشته و در کنار دستگاه کارت خوان و عابر بانک‌ها نصب می‌شود.

سرهنگ اقبالی گفت: کلاهبرداران با توجه به شباهت اسکیمر به دستگاه‌های پوز، این دستگاه را در کنار دستگاه پوز اصلی قرار می‌دهند و در ابتدا کارت خریدار را در دستگاه اسکیمر کشیده که اطلاعات کارت کپی گردیده و به بهانه خراب بودن این دستگاه، کارت خریدار را دوباره در دستگاه پوز اصلی می‌کشند، تا اینجای کار تمام اطلاعات کارت به جز رمز کارت در اختیار کلاهبرداران قرار گرفته و رمز کارت را با روشی بسیار راحت و با پرسش از خریدار که رمزتان چه می‌باشد به دست می‌آورند.

برای پیشگیری از کلاهبرداری اسکیمری خریداران حین خرید با کارت بانکی و انجام عملیات بانکی با دستگاه‌های کارتخوان سیار از در اختیار گذاشتن رمز بانکی خود به دیگران و فروشنده‌ها خودداری کرده و خود اقدام به کشیدن کارت و وارد کردن رمز در دستگاه کارتخوان بانکی بکنند و برای احتیاط بیشتر از عدم اتصال وسیله اضافه‌ای به دستگاه کارتخوان مطمئن شوند و از دستگاه‌کارت‌خوان دوره‌گردها و دست فروش‌ها در حد امکان استفاده نکنید.

ضرورت‌های تامین امنیت دورکاری از سوی کارمندان را جدی بگیریم

دورکاری از طریق اینترنت و در منزل که به عنوان راهکاری برای مقابله با بیماری کرونا به کارگرفته شده؛ دارای تهدیداتی است که کارمندان برای مقابله با این تهدیدات بایستی نکاتی را رعایت کنند. مدیران و کارمندان سازمان‌ها و شرکت‌ها برای افزایش امنیت دورکاری بایستی، استفاده از پل‌های ارتباطی رمزنگاری شده، استفاده از گذر واژه‌های قوی، فعال کردن رمزهای دو مرحله تجهیزات مورد استفاده و حساب‌های کاربری را مد نظر قرار دهند.

به‌روزرسانی به موقع آنتی‌ویروس و نرم‌افزارهای مورد استفاده، پشتیبان‌گیری از اطلاعات مهم و ذخیره در محل‌های قابل اطمینان (هارد اکسترنال وغیره) و عدم استفاده از سایت‌هایی که دارای پروتکل‌های امنیتی نیستند، از جمله مواردی هستند که می‌تواند در جهت بالا بردن امنیت دورکاری از طریق فضای مجازی به کار گرفت.

سازمان‌ها و شرکت‌هایی که کارمندان آنها دورکاری می‌کنند بایستی اقدامات موردنیاز در جهت بالا بردن امنیت کاری از جمله تهیه زیرساخت‌ها و تأمین یک بستر امن و رمزنگاری شده را جدی‌بگیرند.

فیشینگ در قالب ثبت آگهی در دیوار و شیپور

با توجه به ادامه شیوع ویروس کرونا در کشور، بسیاری از شهروندان برای تبلیغ و فروش اجناس و وسایل خود از سایت‌های دیوار و شیپور استفاده می‌کنند و غافل از اینکه مجرمان سایبری برای کلاهبرداری از آنان در کمین نشسته‌اند. بعد از درج آگهی در سایت‌های فروشگاهی، کلاهبرداران با ارسال پیامکی با محتوای "پرداخت مبلغ ناچیز برای درج هزینه آگهی" به کاربرانی که آگهی تبلیغاتی در این سایت درج کرده‌اند، اقدام به ارسال لینک جعلی می‌کنند. لینک معرفی شده در این پیامک‌ها یک درگاه جعلی (فیشینگ) است، کلاهبرداران سایبری با این شگرد مجرمانه، اطلاعات کارت بانکی متقاضیان را به سرقت برده و نسبت به برداشت غیرمجاز از حساب بانکی آنها اقدام می‌کنند.

کلاهبرداران و سودجویان فضای سایبری، سعی دارند تا با شیوه و شگردهای گوناگون اهداف شوم خود را عملی سازند، اما باید این موضوع را مد نظر قرار دهیم که فروشگاه‌های آنلاین به خصوص سایت دیوار هرگز در پیام کوتاه درخواستی برای پرداخت وجه ارسال نمی‌کند؛ درخواست پرداخت خارج از فضای اپلیکیشن و سایت، زمینه‌چینی برای کلاهبرداری است. افراد به ویژه دارندگان مشاغلی که فعالیت‌های زیادی در سایت‌های فروشگاهی دیوار و شیپور دارند برای پیشگیری از برداشت غیرمجاز و وقوع جرایم سایبری نباید فریب پیامک‌های دریافتی را بخورند.

کاربران از باز کردن لینک‌های ارائه شده از سوی افراد ناشناس از طریق شماره تلفن‌های اپراتورهای همراه اول، ایرانسل و رایتل و یا اکانت‌های ناشناس در شبکه‌های اجتماعی جهت درج و تمدید آگهی تبلیغات در سایت‌های دیوار و شیپور اعتماد نکنند، زیرا ممکن است دامی در جهت کلاهبرداری بوده و شما را به درگاه‌های جعلی پرداخت هدایت کنند.

BitNinja
Server Security

مرکز تخصصی آپا دانشگاه رازی