بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و هشتم

دی و بهمن ۱۳۹۹

سلاح جدید هکرها برای حملات مختلف!

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:

مرکز تخصصـــی آپـا دانشگـاه رازی

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

همکاران این شماره:

سهیلا مرادی

صبا آزرمی

سیده مرضیه حسینی

سیده آرزو حسنی

پویا شکری

آدرس:

کرمانشـــاه، باغ ابریشـــم، دانشـــگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

۰۸۳۳۴۳۴۳۲۵۱ apa@razi.ac.ir

@APARazi cert.razi.ac.ir

اخبار امنیتی

مورد حمله قرار گرفتن سیستم‌های ویندوزی و لینوکسی توسط کرم جدید Golang

یک بدافزار مبتنی بر Golang که به تازگی کشف شده و در حال گسترش است، از اوایل دسامبر به طور فعالانه استخراج‌کنندگان رمز ارز XMRig را بر روی سرورهای ویندوزی و لینوکس مستقر می‌کند. این کرم می‌تواند به سرعت انتشار یابد و هدف آن استقرار استخراج‌کننده‌های XMRig در دستگاه‌های آلوده برای استخراج Monero در مقیاس بزرگ می‌باشد. برای دستیابی به این هدف، بدافزار دارای قابلیت‌های Wormable است. این اصطلاح یعنی مجرمان می‌توانند با یک بار نفوذ به یک سیستم مخرب، مجموعه‌ای زنجیره‌وار از حمله‌ها تشکیل دهند که امکان نفوذ از یک ماشین آسیب‌پذیر را به ماشین آسیب‌پذیر بعدی ممکن می‌کند و هیچ نیازی هم به دستوری از طرف ادمین یا کاربر سیستم آلوده ندارد. این بدان معناست که کرم می‌تواند از طریق سرویس‌هایی که در دسترس عموم هستند به ویژه آن‌ها که دارای گذرواژه ضعیف هستند (مانند MySQL، پنل مدیریتی Tomcat و Jenkins) به سایر دستگاه‌ها منتقل شود. در واقع این کرم با اسکن و اجرای Brute-Force بر روی سرویس‌های عمومی نام‌برده، با استفاده از رمز عبور پیش‌فرض و یا لیستی از اطلاعات ورود معتبر، به سایر سیستم‌ها سرایت می‌کند. این در حالی است که نسخه‌های قدیمی‌تر آن می‌توانند از آسیب‌پذیری CVE-2020-14882 که Oracle WebLogic را تحت تأثیر قرار می‌دهد سوءاستفاده کنند. این بدافزار سرورهای ویندوزی و لینوکسی را هدف قرار داده و می‌تواند به راحتی از یک سیستم‌عامل به سیستم عامل دیگر مانور دهد.

تجزیه و تحلیل فنی

این حمله شامل سه مؤلفه است: اسکریپت dropper (به صورت bash یا powershell)، کرم باینری Golang و استخراج‌کننده XMRig (که تمامی آن‌ها در یک سرور C&C میزبانی می‌شوند).

حمله بدین صورت است که بدافزار به محض دست یافتن به سیستم هدف، ابتدا پورت ۵۲۰۱۳ را بررسی می‌کند که آیا پردازشی در دستگاه آلوده روی

این پورت شنود می‌کند یا خیر، وجود شنونده بر روی این پورت به عنوان mutex برای بدافزار عمل می‌کند. اگر دستگاه در حال شنود بر رروی پورت مذکور باشد بدافزار بلافاصله خود را از بین می‌برد، و اگر دستگاه در حال شنود روی این پورت نباشد، بدافزار سوکت شبکه‌ی خود را بر روی این پورت باز کرده و فرآیند آلوده نمودن سیستم را آغاز نموده و کرم و XMRig Miner را در سیستم‌های ویندوزی و لینوکسی مستقر می‌سازد. بدین صورت که به محض تسخیر شدن یکی از سرورهای هدف، اسکریپت‌لودر (ld.sh برای لینوکس و ld.ps1 برای ویندوز) را مستقر می‌کند که هم XMRig Miner و هم کرم باینری مبتنی بر Golang را در سرور وارد می‌کند. لازم به ذکر است که کرم باینری و اسکریپت bash dropper در virustotal قابل شناسایی نیستند.

توصیه امنیتی

کاربران باید اقدامات امنیتی پیشگیرانه را برای جلوگیری از این حمله اتخاذ کنند. بدین منظور اقدامات زیر توصیه می‌گردد:

- از رمزهای عبور پیچیده استفاده کنید ، تلاش برای ورود را محدود کنید و در صورت امکان از 2FA (احراز هویت دو عاملی) استفاده کنید.
- استفاده از سرویس‌های عمومی (مانند MySQL، پنل مدیریتی Tomcat و Jenkins) را کاهش دهید.
- اطمینان حاصل کنید که سرورهای شما از طریق اینترنت قابل دسترسی نیستند.
- نرم‌افزارها را همیشه با آخرین وصله‌های امنیتی را به روز نگه دارید.
- برای مشاهده‌ی زمان اجرای کامل کد در سیستم خود و دریافت پیغام هشدار در صورت وجود هر گونه کد مخرب یا غیرمجاز، از یک Cloud Workload Protection Platform (CWPP) مانند Intezer Protect استفاده کنید.

منبع خبر :

Scan Link

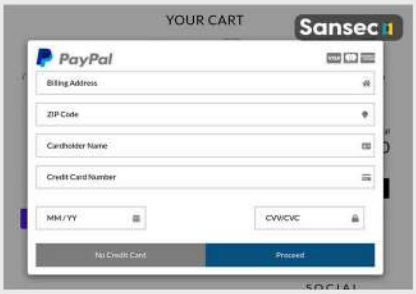
هشدار کارشناسان در رابطه با خطرات اسکیمر نرم‌افزاری در برخی از افزونه‌های فروشگاهی آنلاین

کارشناسان امنیت سایبری، از مشاهده یک اسکیمر نرم‌افزاری کارت اعتباری چندپلتفرمی خبر می‌دهند که به مهاجمان اجازه می‌دهد اطلاعات مربوط به پرداخت را در فروشگاه‌های اینترنتی در معرض خطر، که توسط افزونه‌های Zencart، BigCommerce، Shopify و Woocommerce پیاده‌سازی شده‌اند، به‌دست آورند.

محققان امنیتی Sansec، مشاهده کرده‌اند که این اسکیمر جدید، قادر به برقراری تعامل با مراحل و روند پرداخت در فروشگاه‌هایی است که در آن‌ها از افزونه‌های نام برده شده جهت مدیریت سیستم فروشگاه آنلاین استفاده شده است.

همچنین این نرم‌افزار می‌تواند فروشگاه‌های اینترنتی را که با BigCommerce و Shopify کار می‌کنند ، هدف قرار دهد. در واقع این نرم‌افزار یک فرم پرداخت جعلی را به کاربر نشان می‌دهد، که این فرم برای ضبط کلیدهای وارد شده توسط مشتری قبل از ورود به صفحه واقعی پرداخت طراحی شده است.

افزونه‌های میزبانی صفحات فروشگاهی مانند BigCommerce و Shopify، به طور پیش‌فرض اجازه اجرای کد Javascript سفارشی شده در صفحات پرداخت را نمی‌دهند. این نرم‌افزار با نشان دادن یک فرم پرداخت جعلی و ضبط کلیدهای وارد شده‌ی مشتری قبل از ورود به صفحه اصلی پرداخت، این مانع را دور می‌زند. پس از رهگیری داده‌ها و اطلاعات کاربر، اسکیمر پیغام خطایی را نشان می‌دهد و مشتری به صفحه پرداخت اصلی هدایت می‌شود.



هنگامی که مشتریان اطلاعات کارت اعتباری خود را ارائه دهند، نرم‌افزارخطایی را به کاربر نمایش داده و مشتریان را به صفحه اصلی پرداخت هدایت می‌کند تا از ایجاد سوءظن جلوگیری کند.

این مورد امنیتی به دلیل اینکه بسیاری از افزونه‌های مختلف را هدف قرار داده است، دارای اهمیت بالایی است، زیرا ممکن است مهاجمان موارد مشترک را مورد تهاجم قرار دهند.

همچنین، کارشناسان مطرح کرده‌اند که این اسکیمر چند پلتفرمی، از دامنه‌هایی که توسط برنامه با استفاده از کدگذاری base64 برای تولید یک نام دامنه جدید استفاده می‌شود، برای شکستن فیلترها و موانع استفاده کرده‌اند.

مانند موارد زیر:

- zg9tywlubmftzw5ldza.com
- zg9tywlubmftzw5ldze.com
- zg9tywlubmftzw5ldzu.com
- zg9tywlubmftzw5ldzq.com
- zg9tywlubmftzw5ldzm.com
- zg9tywlubmftzw5ldzy.com
- zg9tywlubmftzw5ldzi.com
- zg9tywlubmftzw5ldzg.com

اولین مورد این دامنه‌ها در تاریخ ۳۱ آگوست سال ۲۰۲۰ به ثبت رسید.

Sansec در این خصوص این نتیجه گیری را مطرح کرده است که: "به طور خلاصه، این مورد نشان می‌دهد که نوع افزونه‌ای که با استفاده از آن، فروشگاه‌های آنلاین پیاده‌سازی شده‌اند، هیچ محدودیتی در کلاهبرداری به روش اسکیمر آنلاین ندارد، و هر کجا که مشتریان جزئیات واطلاعات پرداخت خود را وارد کنند، در معرض خطر قرار می‌گیرند."

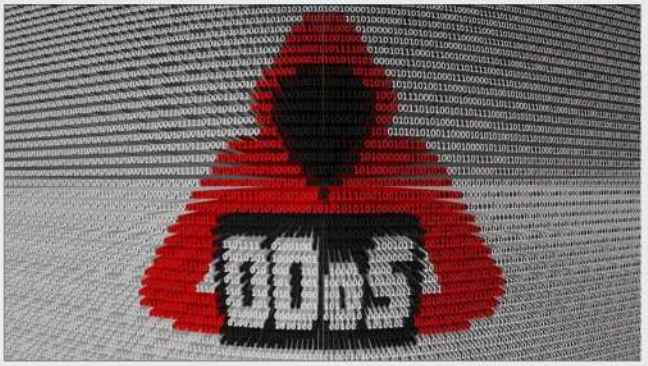
محققان Sansec چندین کمپین Magecart را که از تکنیک‌های جدید دور زدن موانع استفاده می‌کردند، رصد کرده‌است. در اوایل ماه دسامبر، آن‌ها کمپینی را کشف کردند که برای ورود به سیستم، بدافزار را در پرونده‌های CSS مخفی می‌کرد.

کارشناسان چندین روش حمله Magecart را در ماه‌های گذشته مورد تجزیه و تحلیل قرار دادند، که در آن‌ها مهاجمان با پنهان کردن کد مخرب در چندین مؤلفه سایت، از جمله تصاویر و فاکتورها، وب سایت‌ها را به خطر می‌انداختند.

منبع خبر :

Scan Link

باند باج‌افزاری که از حملات DDoS برای باج‌خواهی استفاده می‌کند!



اکنون زمان آن فرارسیده است که مشاغل و سازمان‌ها برای حفاظت از خود در مقابل DDoS سرمایه‌گذاری کنند، چرا که مهاجمان حملات گسترده DDoS را برای اخاذی از سازمان‌ها آغاز کرده‌اند. یک باند باج‌افزاری با استفاده از حملات DDoS، قربانیان را مجبور می‌کند که با آن‌ها تماس بگیرند و برای پرداخت باج مذاکره کنند.

در اکتبر ۲۰۲۰، در رابطه با این باند باج‌افزاری گزارش داده شده بود، که این باند از حملات DDoS بر روی شبکه یا وب‌سایت قربانیان به عنوان اهرم فشار برای پرداخت باج استفاده می‌کند. در آن زمان، SunCrypt و RagnarLocker از این تاکتیک جدید استفاده می‌کردند.

حمله‌ی منع سرویس توزیع شده[1]، یا همان DDoS، حمله‌ای است که در آن، مهاجم، وب‌سایت یا ارتباط شبکه را با سیل درخواست‌ها غرق می‌کند و چون این میزان درخواست بسیار بیشتر از آن است که سیستم می‌تواند کنترل کند، سیستم از دسترس خارج می‌شود.

هنگامی که یک شرکت دچار حمله‌ی باج‌افزاری می‌شود و فایل‌های موجود بر روی سیستم‌ها رمز می‌شوند، بسیاری از قربانیان از نسخه‌ی پشتیبانی که قبلاً تهیه کرده‌اند استفاده می‌کنند و باج خواسته شده را نمی‌پردازند. اما باند باج‌افزاری Avaddon بر خلاف شیوه‌های باج‌خواهی معمول، از حملات DDoS برای از کار انداختن وب‌سایت یا شبکه‌ی قربانی استفاده می‌کند تا قربانی مجبور شود برای دسترسی به وب‌سایت یا شبکه ی خود با مهاجم تماس بگیرد و در خصوص پرداخت باج مذاکره کند. تا زمانی که قربانی با مهاجم تماس نگیرد، شبکه یا وب‌سایت وی به طور مداوم تحت حمله‌ی DDoS است.

ترکیب حملات باج‌افزاری با حملات DDoS اصلاً تعجب‌آور نیست! چرا که انجام حملات DDoS ساده و کم‌هزینه است و در برخی موارد می‌تواند شرکت‌ها را به سرعت متقاعد کند که باج خواسته شده را بپردازند. هر چه فشار وارده بیشتر باشد امکان پرداخت باج توسط قربانی بیشتر است.

مسلماً هنگام بروز چنین رخدادی در شبکه، مقابله با آن دشوار خواهد بود، لذا توصیه می‌گردد پیش از اینکه با این حملات روبرو شوید اقدامات پیشگیرانه را در سازمان و یا مشاغل خود پیاده‌سازی کنید.

منبع خبر :

Scan Link

تقویت حملات DDoS توسط مهاجمان، با بهره‌گیری از سرویس RDP در سرورهای ویندوزی

محققان Netscout بیش از ۱۴۰۰۰ سرور را شناسایی کرده‌اند که می‌توانند توسط مجموعه‌ای از حملات عمومی مورد سوءاستفاده قرار گرفته و شبکه‌ی سازمان‌ها را با سیل ترافیک مواجه کنند.

یافته‌های اخیر در این تحقیقات نشان می‌دهد که مجرمان سایبری می‌توانند از پروتکل RDP مایکروسافت به عنوان یک تقویت‌کننده‌ی قوی برای حملات DDoS استفاده کنند. بدین صورت که مهاجمان می‌توانند از RDP برای انجام حملات UDP reflec-tion/amplification سوءاستفاده کرده و با نسبت ۸۵.۹:۱ حملات DDoS را تقویت نمایند.

RDP بخشی از سیستم‌عامل ویندوز است که یک دسترسی مطمئن را به زیرساخت دسکتاپ مجازی از راه دور (VDI) برای ایستگاه‌های کاری و سرورهای مبتنی بر ویندوز

[1] distributed denial of service

فراهم می‌کند. مدیران سیستم می‌توانند RDP را برای اجرا بر روی TCP port ۳۳۸۹ و یا UDP port ۳۳۸۹ پیکربندی کنند.

با این وجود، تمام سروهای RDP تحت تأثیر این حملات قرار نمی‌گیرند و به گفته‌ی محققان، این امر تنها زمانی امکان‌پذیر است که سرویسRDP بر روی UDP port ۳۳۸۹ فعال شده باشد.

محققان Netscout بیش از ۱۴۰۰۰ سرور RDP قابل سوءاستفاده شناسایی کرده‌اند که می‌توانند توسط حملات DDoS مورد سوءاستفاده قرار گیرند. خبر نگران‌کننده این است که به دلیل شیوع ویروس کرونا، در این مدت استفاده از سرویس RDP جهت مدیریت سرورها به طور چشمگیری افزایش یافته و به تبع آن، این نوع حملات نیز با رشد قابل توجهی روبرو بوده است.

این خطر در اوایل هفته‌ی گذشته برجسته‌تر شد، زمانی که محققان یک نوع بدافزار جدید به نام Freakout را شناسایی کردند. این بدافزار endpointها را به یک باتنت اضافه می‌کند تا سیستم‌های لینوکسی را برای اجرای حملات DDoS مورد هدف قرار دهد.

در حالی که، در ابتدا تنها مهاجمانی که به زیرساخت‌های حمله‌ی DDoS دسترسی داشتند از این روش تقویت استفاده می‌کردند، اما محققان طی تحقیقات خود مشاهده کردند که از سرورهای RDP نیز در سرویس‌های DDoS-for-hire که به اصطلاح "booters" نامیده می‌شود استفاده می‌شود. این بدان معناست که مهاجم می‌تواند از این حالتِ تقویت، برای افزایش شدت حملات DDoS خود استفاده کند.

مهاجمان می‌توانند ترافیک حمله‌ی تقویت‌شده را که از پکت‌های UDP قطعه‌قطعه‌نشده تشکیل شده است و از UDP port ۳۳۸۹ نشئت می‌گیرد برای یک آدرس IP خاص و پورت UDP انتخابی ارسال کنند و آن را هدف حمله قرار دهند. پکت‌های تقویت‌شده در مقایسه با ترافیک معمولیRDP، ۱۲۶۰ بایت طول دارند و عمده‌ی بایت‌های آن‌ها را رشته‌های طولانی صفر تشکیل می‌دهد.

به گفته‌ی محققان، استفاده از سرورهای RDP بدین شیوه، پیامدهای قابل توجهی برای سازمان‌های قربانی در پی دارد، به عنوان مثال، قطع جزیی یا کلی سرویس‌های حیاتی که از راه دور در دسترس هستند، همچنین ایجاد اختلال در سایر سرویس‌ها به دلیل مصرف ظرفیت انتقال و سایر اثرات مرتبط با آن در زیرساخت شبکه.

محققان خاطرنشان کردند: "فیلتر کردن تمام ترافیک UDP/۳۳۸۹-sourced به صورت یکجا توسط اپراتورهای شبکه، ممکن است موجب مسدودسازی بیش از حد ترافیک مجاز اینترنت مانند پاسخ‌های RDP sessionها از راه دور شود."

به منظور کاهش استفاده از RDP برای تقویت حملات DDoS و سایر پیامدهای مربوط به آن، توصیه‌های زیر پیشنهاد می‌گردد:

- قبل از هر چیز، ابتدا باید سرورهای ویندوزی پشت VPN قرار گیرند، به گونه‌ای که سرویس RDP در آن‌ها تنها از طریق VPN قابل دسترسی باشد.
- اپراتورهای شبکه می‌بایست سرورهای RDP قابل سوءاستفاده را در شبکه‌های خود و یا درشبکه‌های مشتریان زیردست خود شناسایی کنند.
- اگر انجام موارد فوق امکان‌پذیر نیست، حداقل اقدام ممکن این است که مدیران سرور دسترسی به RDP را از طریق UDP port ۳۳۸۹ غیرفعال نمایند.
- ترافیک اینترنت پرسنل سازمانی را از ترافیک اینترنت عمومی تفکیک شود.
- برای دسترسی به زیرساخت شبکه در سازمان، سیاست‌های خاص در نظر گرفته شود. به عنوان مثال، تنها ترافیک‌های دریافتی از IPها و پورت‌های مورد نیاز پذیرش شوند.

منبع خبر :

Scan Link

اخبار کوتاه

هشـــدار در خصـوص ۳ آسیب‌پذیری امنیتی روز صـــفر در سیستم‌عامل iOS

چند روز گذشته شرکت اپل به روزرسانی‌هایی را برای محصولات خود با سیستم‌عامل iOS، iPadOS ، و tvOS جهت رفع سه آسیب پذیری امنیتی منتشر کرد. بر اساس گفته‌های آن شرکت ممکن است این نقص‌ها توسط مجرمان سایبری به طور بالقوه مورد سوءاستفاده قرار گرفته باشد.

به گزارش یک محقق ناشناس، سه نقص امنیتی معروف به روز صفر CVE-2021-1870، CVE-2021-1782 و CVE-2021-1871 بـــرای مهاجمین مجوزهای مؤثری را برای اجرای کدهای دسترسی و کنترل از راه دور فراهم کرده است. سازندگان آیفون میزان گسترده حملات و یا هویت افرادی که مهاجمان از آن‌ها سوءاستفاده می کردند را فاش نکرد.

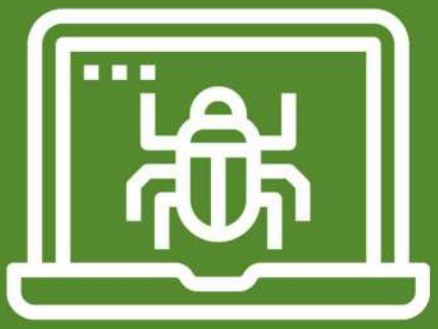
در حالی که وجود نقص شدید امنیتی (CVE-2021-1782) در هسته سیستم‌عامل به عنوان شرایطی ذکر شده که می‌تواند نقش مؤثری در افزایش تأثیرگذاری یک برنامه مخرب داشته باشد، دو نقص امنیتی دیگر (CVE-2021-1870 و CVE-2021-1871) به عنوان "مسئله منطقی" در موتور رندر WebKit کشف شده، که به مهاجم مجوز اجرای خودسرانه کدهای مخرب را در داخل برنامه Safari ارائه می‌دهد.

در حال حاضر بروزرسانی‌های لازم برای تلفن هوشمند آیفون 6S و بالاتر ، iPad Air 2 به بعد ، iPad mini 4 بالاتر، و iPod touch (نسل ۷) و همچنین Apple TV 4K و Apple TV HD در دسترس کاربران می‌باشند.

اکنـــون Microsoft Defender آسیب‌پذیـــری‌هـــای برنامه‌های macOS را شناسایی می‌کند.

مایکروسافت اعلام کرد که Defender for Endpoint اکنون به مدیران کمک خواهد کرد تا آسیب‌پذیری سیستم‌عامل و نرم‌افزار را که بر دستگاه‌های macOS در شبکه سازمانشان تأثیر می‌گذارد کشف کنند.

با ویژگی تهدید و مدیریت آسیب‌پذیری سکوی امنیتی نقطه پایانی سازمانی که اکنون به طورکلی برای macOS در دسترس است، سرپرستان امنیتی می‌توانند ناحیه حمله سطحی نقاط انتهایی را کاهش دهند و بنابراین میزان مقاومت سازمان خود را در برابر حملات ورودی افزایش دهند. مدیر ارشد محصولات مایکروسافت، تومر رایزنر گفت: "این توسعه قابلیت، سازمان‌ها را قادر می‌سازد تا آسیب‌پذیری‌های نرم‌افزار و سیستم‌عامل را در دستگاه‌های دارای macOS کشف، اولویت‌بندی و اصلاح کنند."



آسیب پذیری

هشدار گوگل در خصوص آسیب‌پذیری‌های بحرانی در اندروید

گوگل در بروزرسانی امنیتی خود ۴۳ آسیب‌پذیری که دستگاه‌های اندرویدی، از جمله گوشی‌های سامسونگ را تحت تأثیر قرار می‌دهد برطرف نمود.

گوگل دو آسیب‌پذیری بحرانی را بر روی گوشی‌های اندرویدی خود برطرف نمود. این نقص‌ها در مؤلفه‌ی Android System وجود دارند و به مهاجم از راه دور اجازه می‌دهند تا کد دلخواه خود را بر روی دستگاه آسیب پذیر اجرا کند.

این بروزرسانی امنیتی به طور کلی ۴۳ آسیب‌پذیری را در سیستم‌عامل‌های اندروید خود برطرف نمود. این نقص‌ها در مؤلفه‌ی Android System وجود دارند و به مهاجم از راه دور اجازه می‌دهند تا کد دلخواه خود را بر روی دستگاه آسیب‌پذیر اجرا کند.

این بروزرسانی امنیتی به طور کلی ۴۳ آسیب‌پذیری را در سیستم‌عامل‌های اندروید برطرف کرده است. به عنوان مثال، برای کوالکام که تراشه‌های آن در دستگاه های اندرویدی استفاده می‌شوند، ترکیبی از آسیب‌پذیری‌های با شدت بحرانی و بالا که شامل ۱۵ آسیب‌پذیری می‌باشند وصله شده است.

آسیب‌پذیری‌های بحرانی شامل نقص اجرای کد از راه دور (با شناسه CVE-2021-0316) در مؤلفه‌ی Android System گوگل _هسته‌ی اصلی سیستم‌عامل اندروید_ و نقص دیگر، مشکل منع سرویس (با شناسه CVE-2021-0313) در مؤلفه‌ی Android Framework _مجموعه‌ای از APIها، متشکل از ابزارهای سیستم و ابزارهای طراحی رابط کاربرکه به توسعه‌دهندگان اجازه می‌دهد تا به سرعت و به راحتی برای تلفن‌های اندرویدی برنامه بنویسند_ می‌باشد.

به گفته‌ی گوگل، شدیدترین این موارد، آسیب‌پذیری امنیتی با شدت بحرانی در مؤلفه‌ی System است که مهاجم از راه دور را قادر می‌سازد تا با یک transmission ساختگی کد دلخواه خود را در چارچوب یک پردازش دارای سطح دسترسی بالا اجرا نماید. هر دوی این آسیب‌پذیری‌ها در اندروید نسخه‌ی ۸.۰، ۸.۱، ۹، ۱۰ و ۱۱ برطرف شده‌اند.

علاوه بر این نقص‌ها که دارای شدت بحرانی می‌باشند، گوگل ۱۳ نقص با شدت بالا را نیز در Framework خود برطرف نموده است که شامل ۸ نقص مربوط به ارتقاء سطح دسترسی (CVE-2021-0307, CVE-2021-0306, CVE-2021-0303, CVE-2021-0317, CVE-2021-0315, CVE-2021-0310, CVE-2021-0319, CVE-2021-0318)، ۴ نقص مربوط به افشای اطلاعات (CVE-2021-0321, CVE-2021-0309, CVE-2021-0304, CVE-2021-0322) و یک نقص منع سرویس (CVE-2019-9376) می‌باشد.

سه آسیب‌پذیری با شدت بالا نیز در Media Framework _که پشتیبانی از پخش انواع رسانه‌های رایج را پشتیبانی می‌کند و بنابراین کاربران می‌توانند به راحتی از صدا، ویدئو و تصاویر استفاده کنند_ یافت شده است. این موارد شامل یک نقص RCE مربوط به CVE-2016-6328، و دو نقص افشای اطلاعات مربوط به CVE-2021-0311 و CVE-2021-0312 می‌باشند.

گوگل همچنین اصلاحاتی را برای نقص در اجزای شخص ثالث مختلف در اکوسیستم اندروید خود ارائه داده است، که شامل سه نقص در هسته (CVE-2020-10732، CVE-2021-0323، CVE-2020-10766) است، که می‌تواند یک برنامه مخرب محلی را قادر سازد که مکانیزم محافظتی سیستم‌عامل را _که داده‌های برنامه را از برنامه‌های دیگر مجزا می‌کند _ دور بزند. علاوه بر این، یک آسیب‌پذیری با شدت بالا (CVE-2021-0301) نیز در مؤلفه‌ی MediaTek برطرف شد.

سرانجام، ۱۵نقص با شدت بحرانی و بالا در اجزای کوالکام، از جمله مواردی که بر هسته (CVE-2020-11233)، صفحه‌نمایش (CVE-2020-11239، CVE-2020-11262، CVE-2020-11261)، دوربین (CVE-2020-11240) و اجزای صوتی (CVE-2020-11250) تأثیر می‌گذارند مرتفع گردید.

آسیب‌پذیری‌های مذکور در بروزرسانی امنیتی اندروید در ماه دسامبر برطرف شده‌اند. به کاربران دستگاه‌های اندرویدی توصیه می‌شود آخرین بروزرسانی‌های ارائه شده توسط گوگل را نصب نمایند.

منبع خبر :

Scan Link

این آسیب‌پذیری با شناسه CVE-2020-29583 و شدت بالا (۷.۸ از ۱۰)، در واقع یک آسیب پذیری تأیید اعتبار hardcode، در حساب کاربری "zyfwp"، در برخی از فایروال‌ها و AP کنترلرهای Zyxel شناسایی شده است. رمز ورود به این حساب را می‌توان در clear text موجود در فریمورها پیدا کرد. مهاجم می تواند از این حساب برای ورود ssh به سرور یا رابط وب، با امتیازات و دسترسی مدیر استفاده کند. این حساب به منظور ارائه بروزرسانی خودکار فریمورها برای اتصال به access point ها از طریق FTP طراحی شده است.

این آسیب‌پذیری نسخه‌های زیر از فایروال‌ها و AP کنترلرها را تحت تاثیر قرار می‌دهد. توجه داشته باشید که فایروال‌های USG FLEX ، USG ،ATP و VPN که نسخه‌های اولیه فریمور را اجرا می‌کنند و سری VPN که دارای SD-OS هستند، تحت تأثیر این آسیب‌پذیری قرار نمی‌گیرند.

- ATP series running firmware ZLD V4.60
- USG series running firmware ZLD V4.60
- USG FLEX series running firmware ZLD V4.60
- VPN series running firmware ZLD V4.60
- NXC2500
- NXC5500

این آسیب‌پذیری هنگام انجام تحقیقات (روت کردن) روی Zyxel USG40، شناسایی شد. محقق امنیتی شرکت EYE از یافتن حساب کاربری "zyfwp" با رمز عبور hash شده، در آخرین نسخه فریمور (۴.۶۰) خبر داد. متن رمز عبور در یکی از باینری فایل‌های سیستم به صورت ساده و رمز نشده، قابل مشاهده بود.

همچنین این حساب هم بر روی SSH و هم رابط وب قابل استفاده بود. از آنجا که کاربر zyfwp دارای امتیازات و دسترسی مدیر است، این مورد یک آسیب‌پذیری جدی به‌شمار می‌رود. یک مهاجم می‌تواند محرمانه بودن و در دسترس بودن دستگاه را به خطر بیندازد. به عنوان مثال می‌تواند تنظیمات فایروال را تغییر دهد تا ترافیک خاصی را مجاز یا مسدود کند. آنها همچنین می‌توانند برای دسترسی به شبکه پشت دستگاه، ترافیک را رهگیری کرده یا حساب های VPN ایجاد کنند.

حدود ۱۰٪ از دستگاه‌ها همچنان نسخه‌های آسیب‌پذیر را اجرا می‌کنند. از کاربران خواسته شده، نسخه فریمور خود را در اسرع وقت به جدیدترین نسخه به‌روز کنند.

پس از بررسی‌های دقیق، کارشناسان محصولات آسیب پذیر را شناسایی کرده و در حال انتشار وصله های فریمور برای حل این مشکل هستند، همانطور که در جدول زیر نشان داده شده است، برای محافظت از محصولات و خدمات از کاربران خواسته شده وصله‌های به‌روز را نصب کنند.

پس از بررسی‌های دقیق، کارشناسان محصولات آسیب پذیر را شناسایی کرده و در حال انتشار وصله های فریمور برای حل این مشکل هستند، همانطور که در جدول زیر نشان داده شده است، برای محافظت از محصولات و خدمات از کاربران خواسته شده وصله‌های به‌روز را نصب کنند.

برای رفع آسیب‌پذیری‌های مذکور بروزرسانی به نسخه‌های زیر توصیه می‌گردد:

[۱] فرآیند تبدیل جریان بایت به داده

[۲] اگرچه HPE SIM هر دو سیستم‌عامل ویندوز و لینوکس را پشتیبانی می‌کند، اما در حال حاضر، تنها راهکار کاهش خطر در سیستم‌های ویندوزی توسط شرکت HPE ارائه شده است.

- ATP series running firmware ZLD V4.60 ➡ ZLD V4.60 Patch1 in Dec. 2020
- USG series running firmware ZLD V4.60 ➡ ZLD V4.60 Patch1 in Dec. 2020
- USG FLEX series running firmware ZLD V4.60 ➡ ZLD V4.60 Patch1 in Dec. 2020
- VPN series running firmware ZLD V4.60 ➡ ZLD V4.60 Patch1 in Dec. 2020
- NXC2500 ➡ V6.10 Patch1 in April 2021
- NXC5500 ➡ V6.10 Patch1 in April 2021

منبع خبر :

Scan Link

آسیب‌پذیری سرریز بافر هیپ در Sudo

این آسیب‌پذیری با شناسه CVE-2021-3156 و شدت بالا (۷.۸ از ۱۰)، در واقع یک آسیب‌پذیری سرریز بافر هیپ در ابزار Sudo، که به هر کاربر محلی اجازه می‌دهد بدون احراز هویت به عنوان کاربر root، در سیستم‌های لینوکسیِ آسیب‌پذیر دسترسی root بگیرد. Sudo _مخفف Superuser do_ یک قابلیت پیش‌فرض در اکثر توزیعات لینوکس و سیستم‌عامل‌های مبتنی بر یونیکس است که به کاربران اجازه می‌دهد دستورات را به عنوان کاربر root اجرا کنند. بنابراین، این حمله شامل ارتقاء سطح دسترسیِ غیرمجاز با سوءاستفاده از قابلیت سودمند لینوکس می‌باشدکه به دلیل سرریز بافر هیپ اتفاق می‌افتد و از مدیریت نادرست بک‌اسلش‌ها در آرگومان‌های دستور ناشی می‌شود. در واقع، Sudo نمی‌تواند تجزیه‌ی پارامترهای دستور را به درستی انجام دهد.

از آنجا که ابزار Sudo نمی‌تواند پارامترهای دستور را به درستی تجزیه و مدیریت کند، اگر آرگومانِ خط فرمان با بک‌اسلش (\) خاتمه یابد _مانند دستور sudo make me a\ sandwich_ آنگاه کامپیوتر فراتر از بک‌اسلش را می‌خواند (کاراکترِ موردِ انتظار بعدی) و کاراکترِ خارج از محدوده را در بافر کپی می‌کند. این امر به مهاجم اجازه می‌دهد تا حافظه را با هر اندازه بافر که می‌خواهد بازنویسی کند. از لحاظ تئوری مهاجم نباید بتواند از این طریق حافظه‌ی هیپ را با داده‌های دلخواه بازنویسی کند، اما اجرای Sudo با i- یا s- موجب شود به طور خودکار از کاراکترهای خاصی که همراه بک‌اسلش می‌آیند صرف نظر شود. بنابراین، با یک بک‌اسلش دیگر مانند \\، از بک‌اسلش صرف‌نظر می‌شود و در نتیجه، سیاست امنیتی کاربران Sudoer که مشخص می‌کند چه کاربرانی چه دستوراتی می‌توانند اجرا کنند، پیش از آنکه مورد بررسی قرار گیرد با یک کاراکتر خاص نادیده گرفته می‌شود.

این آسیب‌پذیری، تمام نسخه‌های قدیمی Sudo (از ۱.۸.۲ تا ۱.۸.۳۱p۲) و تمام نسخه‌های پایدار آن (از ۱.۹.۰ تا ۱.۹.۵p۱) را تحت تأثیر قرار می‌دهد.

روش شناسایی

با انجام مراحل زیر می‌توان سیستم آسیب‌پذیر را شناسایی نمود:

۱. با یک کاربر غیر root به سیستم وارد شوید.

۲. دستور sudoedit -s / را اجرا کنید.

۳. اگر سیستم آسیب‌پذیر باشد، در پاسخ خطایی بازگردانده می‌شود که با "sudoedit:" شروع می‌شود.

۴. اگر سیستم وصله شده باشد و آسیب‌پذیر نباشد، در پاسخ خطایی بازگردانده می‌شود که با "Usage:" شروع می‌شود.

توصیه امنیتی

آسیب‌پذیری مذکور در Sudo نسخه‌ی ۱.۹.۵p۲ برطرف شده است. به کاربران توصیه می‌شود در اسرع وقت ابزار Sudo را به نسخه‌ی توصیه شده بروزرسانی نمایند.

منبع خبر :

Scan Link

آسیب‌پذیری سرریز بافر در پایتون

این آسیب‌پذیری با شناسه CVE-2021-3177 و شدت بالا، یک آسیب‌پذیری سرریزِ بافرِ مبتنی بر پشته در تابع PyCArg_repr از ماژول ctypes، که در برنامه‌های کاربردی خاصی که به زبان پایتون نوشته شده‌اند و اعداد شناور را به عنوان ورودی غیرقابل اعتماد می‌پذیرند می‌تواند منجر به اجرای کد از راه دور شود. دلیل این امرآن است که تابع sprintf به صورت ناامن مورد استفاده قرار می‌گیرد. این آسیب‌پذیری فاکتور "دسترس‌پذیری" از فاکتورهای سه‌گانه‌ی امنیت را تحت تأثیر قرار می‌دهد.

این آسیب‌پذیری به دلیل عدم اعتبارسنجی دقیق ورودی در تابع PyCArg_repr به

وجود می‌آید. یک مهاجم از راه دور می‌تواند با دادن ورودی‌های ساختگی به برنامه‌های کاربردی که اعداد شناور را به عنوان ورودی غیرقابل اعتماد می‌پذیرند، و سرریز کردن بافر بر روی پشته، موجب از کار افتادن برنامه کاربردی، خرابی حافظه و اجرای کد از راه دور در سیستم هدف شود.

روش شناسایی

برنامه‌های کاربردی که از ماژول ctypes بدون اعتبارسنجی دقیقِ ورودی استفاده می‌کنند می‌توانند آسیب‌پذیر باشند.

در حال حاضر راهکار کاهش یا رفع آسیب‌پذیری توسط پایتون ارائه نشده است.

منبع خبر :

Scan Link

آسیب‌پـــذیری روز صفـــر در مرورگر Google Chrome

اخیراً شرکت گوگل بروزرسانی امنیتی برای آسیب‌پذیری روز صفر مرورگر گوگل کروم با شناسه CVE-2021-21148 در سیستم‌عامل‌های ویندوز، مک و لینوکس منتشر کرد. آسیب‌پذیری مذکور، به صورت گسترده مورد بهره‌برداری قرار گرفته است. این نقص امنیتی، مربوط به سرریز پشته در موتور جاوااسکریپت V8 می‌باشد که یک مفسر بسیار سریع جاوااسکریپت است که در مرورگر کروم اجرا می‌شود. پس از بررسی‌های صورت گرفته توسط محققان، آن‌ها به این نتیجه رسیدند که این مسئله یک نقص Double Free است که در بخشی از ویژگی شیء DOM وجود دارد. با این وجود از API (رابط برنامه نویسی نرم‌افزار) موجود در این آسیب‌پذیری جهت انتشار داده‌های رشته‌ای متصل به شیء DOM استفاده می‌شود.

در صورت اجرای Control Flow Guard در کد حمله، می‌توان از مکانیزم RPC توسط سیستم‌عامل ویندوز جهت انتقال APIهای دلخواه بهره‌برداری کرد. shellcode به سادگی یک لیست از فرآیندهایی که بر روی سیستم تحت تأثیر این آسیب‌پذیری در حال اجرا هستند، ارسال کرده و از این طریق تمام اطلاعات مورد نظر را از سیستم آلوده، دریافت خواهد کرد. سپس کد مخرب رمزگذاری شده‌ی دیگری را از سرور C2 بر روی حافظه اجرا می‌کند.

تمام نسخه‌های قبل از نسخه ۸۸.۰.۴۳۲۴.۱۵۰ آسیب‌پذیر هستند.

توصیه امنیتی

کاربران هر چه سریع‌تر مرورگر گوگل کروم خود را به نسخه ۸۸.۰.۴۳۲۴.۱۵۰ ارتقاء دهند. این بروزرسانی امنیتی برای سیستم‌عامل‌های ویندوز، مک و لینوکس ارائه شده است. مراحل اعمال بروزرسانی به صورت زیر می‌باشد:

Chrome menu –> Help –> About Google Chrome

منبع خبر :

Scan Link

اخبار کوتاه

در صورت به خطر افتادن رمزهای شما، Microsoft Edge به شما اطلاع می دهد!

Edge این کار را به این منظور انجام می دهد که مانع دیدن مدارک شما توسط کسی شود. حتی اگر از رمز عبور و احراز هویت دو عاملی استفاده می کنید، به دلیل هک ها و درزها، احتمالاً برخی از اطلاعات ورود به سیستم شما در گذشته نشان داده شده است.

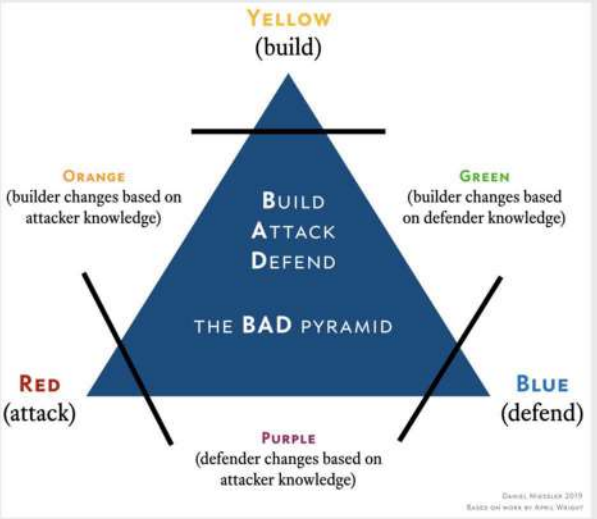
مایکروسافت در حال معرفی ویژگی جدیدی به Edge به نام Password Monitor است. بنابراین شما نیازی به مراجعه به وب‌سایت دیگری ندارید تا متوجه شوید یکی از رمزهای عبور شما به خطر افتاده است.

پس از اینکه این قابلیت فعال شود، مرورگر به‌صورت خودکار امنیت گذرواژه‌های تعریف شده را بررسی می‌کند و اگر هر کدام از آن‌ها به شیوه‌های مختلف در خطر قرار بگیرد، با ارسال پیام به کاربر هشدار می‌دهد. به این ترتیب، می‌توانید هرگونه آسیب احتمالی را به حداقل برسانید؛ به‌ویژه اگر از یک رمز عبور برای حساب‌های مختلف استفاده کرده باشید. Firefox، Chrome و همچنین مدیران گذرواژه مانند 1Password و LastPass از چند سال گذشته عملکرد مشابهی ارائه داده‌اند.

با این حال، آنچه پیشنهاد مایکروسافت را جذاب می کند این است که از نوع نسبتاً جدیدی به نام رمزگذاری هومومورفیک استفاده می کند تا اطمینان حاصل کند که هیچ‌کس در این شرکت یا هیچ طرف دیگری نمی تواند رمزهای ورود شما را پیدا کند. یکی از راه هایی که الگوریتم از داده‌های شما محافظت می کند این است که به رایانه اجازه می‌دهید بدون رمزگشایی اطلاعات با آن ارتباط برقرار کند. همچنین با انواع ماشین‌آلات از جمله دستگاه‌هایی با پردازنده مرکزی نسبتاً قدیمی کار می‌کند تا هر کسی بتواند از رمز عبور مانیتور استفاده کند.

مقالات آموزشی

تفاوت بین تیم‌های قرمز، آبی و بنفش در امنیت اطلاعات سایبری (بخش اول)



در مورد تعاریف تیم‌های قرمز، آبی و بنفش در امنیت اطلاعات سردرگمی وجود دارد. در اینجا تعاریف و مفاهیم مرتبط با آن‌ها آورده شده است.

تعاریف تیم‌ها:

تیم قرمز(Red Teams): تیم قرمز، تیم آموزش دیده‌ای از متخصصان امنیت خارج و یا داخل سازمان است که هدف آن‌ها یافتن آسیب‌پذیری‌های امنیتی سازمان و مشخص کردن نقاطی است که در آن‌ها ضعف امنیتی وجود دارد. این تیم با استفاده از شبیه‌سازی حملات واقعی به‌صورت مستمر در سطوح مختلف امنیتی، شبکه را تست و سعی در نفوذ به آن را دارند. سازمان‌ها می‌توانند با شبیه‌سازی حملات دنیای واقعی و تمرین تدابیر امنیتی، تکنیک‌ها و روش‌هایی که معمولاً مهاجمان از آن‌ها بهره می‌برند، خود را برای حملات واقعی آماده سازند. در واقع این گروه‌ها وظیفه شناسایی، جلوگیری و از بین بردن آسیب‌پذیری‌ها را دارند.

تیم آبی(Blue Teams): تیم آبی شباهت زیادی به تیم قرمز(Red team) دارد زیرا همانند تیم قرمز امنیت شبکه را ارزیابی کرده و نقاط آسیب‌پذیر شبکه را شناسایی و هرگونه آسیب‌پذیری احتمالی را شناسایی می‌کند. اما این تیم علاوه بر ارزیابی شبکه و به دست آوردن نقاط آسیب‌پذیر، وظیفه یافتن راه‌کارهای دفاعی، تغییر مکانیسم‌های دفاعی یا ایجاد دوباره آن‌ها را در سازمان دارد. تیم آبی در کنار مهارت‌های فوق بایستی دارای مهارت‌های تجزیه و تحلیل و دانش تشخیص نفوذ در شبکه را دارا باشند.

تیم بنفش(Purple Teams): تیم بنفش مفهومی برای توضیح یک تیم نیست بلکه ترکیبی از دو تیم Red team و Blue team به منظور تلفیق تاکتیک‌های دفاعی و کنترل‌های تیم آبی با تهدیدات و آسیب‌پذیری‌های تیم قرمز در یک موضوع یکسان است. زیرا تیم بنفش هر دو تیم را مجبور می‌کند تا با یکدیگر همکاری کنند. شرکت‌ها به مشارکت هر دو تیم با یکدیگر نیاز دارند تا یک بازرسی کامل را با توجه به لاگ‌های هر تست و سوابق مربوطه که ثبت کرده‌اند، انجام دهند. تیم قرمز اطلاعات کسب شده از

عملیاتی که در حین انجام ارزیابی امنیتی به دست آورده‌اند را ارائه می‌دهند و تیم آبی اسنادی را در مورد اقداماتی که برای رفع شکاف‌ها و رسیدن به آسیب‌پذیری‌ها و ضعف‌ها انجام داده‌اند را ارائه می‌دهند. درنتیجه هر دو تیم ضروری هستند. بدون اقدامات این دو تیم سازمان‌ها و شرکت‌ها از نقص‌های امنیتی خودآگاه نخواهند شد. در حالت ایده آل تیم بنفش اصلاً نباید یک تیم باشد بلکه باید یک پویایی دائمی بین تیم قرمز و تیم آبی باشد.

مهارت تیم‌ها:

مهارت‌های تیم قرمز (Red team):

- تفکر خارج از یک چارچوب: به معنی یافتن ابزارها و فن‌های جدید برای محافظت بهتر و قوی‌تر سازمان‌ها به‌طور مداوم است.
- دانش عمیق سیستم‌ها: Red team با داشتن درک کامل از تمام بخش‌ها و سیستم‌ها به شما اجازه تا راه‌های بیشتری برای کشف آسیب‌پذیری‌ها پیدا کنید.
- توسعه نرم‌افزارها: این روش به Red team کمک می‌کند تا بهترین فن‌ها و نرم‌افزارهای را در شبیه‌سازی خود استفاده کنند.
- تست نفوذ
- مهندسی اجتماعی: در حین انجام بررسی‌های دقیق در هر سازمان، دست‌کاری افراد سازمان ممکن است منجر به‌قرار گرفتن اطلاعات در معرض خطر شود، این روش موجب جلوگیری از این احتمالات می‌شود.

مهارت‌های تیم آبی (Blue team):

- جزئی‌گرا و سازمان‌یافته: این روش برای جلوگیری و شناسایی شکاف‌ها در زیرساخت‌های امنیتی شرکت موردنیاز است.
- تجزیه‌وتحلیل امنیت سایبری
- فن‌های امن‌سازی:(Hardening) این فن به معنای ایمن و مقاوم‌سازی سیستم موردنظر است.
- دانش سیستم‌های تشخیص نفوذ: به معنی آشنایی با نرم‌افزارهایی است که امکان ردیابی فعالیت‌های غیرمعمول و مخرب را دارد.

اخبار کوتاه

کلاهبـــرداری با اپلیکیشـــن جـــعلی هـــمراه بـــانک!

پلیس فتا از شناسایی شخصی که با ساخت اپلیکیشن جعلی همراه بانک یکی از بانک‌های رسمی کشور اقدام به سرقت یک میلیارد و ۵۵۰ میلیون ریال از حساب‌های هم‌وطنان کرده، خبر داد. با انجام تحقیقات لازم و در پی بررسی‌های صورت گرفته مشخص شد فرد قربانی برای نصب نرم‌افزار همراه بانک بروزرسانی شده یکی از بانک‌های رسمی کشور در موتور جست‌وجوگر گوگل اقدام به جست‌وجو کرده و پس از مشاهده و دانلود اولین لینک نرم‌افزار که مشابه نرم‌افزار اصلی بانک بوده، به صورت ناآگاه نرم‌افزار مخرب را بر روی تلفن همراه خود نصب کرده و در دام سارقان اینترنتی گرفتارشده است. با توجه به شیوه‌های گوناگون و نوین کلاهبرداران و سارقان اینترنتی در انجام اعمال مجرمانه و خرابکارانه خود به این موضوع توجه داشته باشید که دانلود نرم‌افزار را تنها از مارکت‌های معتبر یا سایت اصلی بانک انجام دهند و به هیچ‌وجه از موتورهای جست‌وجوگر استفاده نکنید.

اخبار داخلی

همایش رایگان آشنایی با کنترل های امنیت اطلاعات در صنعت مالی اعتباری

به دلیل وجود چالش‌های امنیت اطلاعات در حوزه مالی اعتباری، در مورخ ۲ دی ماه ۱۳۹۹ همایش آشنایی با کنترل های امنیت اطلاعات در صنعت مالی اعتباری توسط مرکز آپا دانشگاه رازی برگزار گردید. در این رویداد ضمن آشنایی با ساختار استاندارد امنیت اطلاعات، کنترل‌های امنیت اطلاعات در حوزه مالی به منظور افزایش امنیت داده ها معرفی شد تا شناختی از این کنترل‌ها برای مخاطب ایجاد گردد. استاندارد ISO/IEC TR 27015 کنترل‌های خاص حوزه مالی را برای ایجاد امنیت اطلاعات ارائه شد و برای کاهش مخاطرات این حوزه از منظر امنیت اطلاعات راه‌کارهایی را در غالب این کنترل‌ها برای شرکت کنندگان اعم از دانشجویان، پرسنل IT برخی سازمان‌ها و شرکت‌ها و علاقمندان این حوزه ارائه گردید.

وبینار رایگان تکنیک‌ها و روش‌های نفوذ به شبکه‌های اجتماعی و نحوه مقاوم سازی آن

پلتفرم شبکه های اجتماعی، بسیار محبوب و پر بازدید توسط افراد مختلف است، به همین دلیل یکی از اهداف مهم مجرمان اینترنتی برای بدست آوردن اطلاعات یا کارهای دیگرشان، این شبکه‌ها هستند. از این رو حفظ امنیت در شبکه های اجتماعی بسیار مهم

و قابل توجه می‌باشد. در همین راستا مرکز تخصصی آپا دانشگاه رازی اقدام به برگزاری وبینار رایگان تکنیک‌ها و روش‌های نفوذ به شبکه‌های اجتماعی و نحوه مقاوم سازی آن در مورخ ۱۷ دی ماه ۱۳۹۹ با شرکت علاقمندان در این زمینه نمود.

وبینار رایگان شکار تهدیدات سایبری

شکار تهدیدات سایبری به معنای جستجوی پیش‌کنشانه برای یافتن تهدیدات امنیتی است که بدون شناسایی در یک شبکه موجودند. زمانی که یک برنامه مخرب از شناسایی شدن ابتدایی می‌گریزد و به لایه‌ی دفاعی شبکه نفوذ می‌کند، بسیاری از شرکت‌ها فاقد قابلیت‌های پیشرفته تشخیص تهدیدی هستند که برای پایان دادن به حضور این تهدیدات پیشرفته مورد نیاز است. به همین دلیل شکار تهدیدات بخش جدایی ناپذیری از استراتژی دفاعی به شمار می‌رود.

این وبینار در تاریخ ۸ بهمن ۱۳۹۹ توسط مرکز تخصصی آپا دانشگاه رازی برگزار شد.

هم‌اندیشی رایگان نقشه راه ورود به دنیای جذاب استانداردهای مدیریت امنیت اطلاعات ، شبکه ، امنیت شبکه و امنیت سایبری

همیشه علاقمندان برای ورود به دنیای شبکه، امنیت سایبری و سایر حوزه‌ها با مشکلات زیادی از جمله پیش نیاز دوره‌های، خروجی، کاربرد دوره‌ها و غیره برای گذراندن دوره‌های تخصصی مواجه هستند. در همین راستا رویداد هم‌اندیشی رایگان نقشه راه ورود به دنیای جذاب استانداردهای مدیریت امنیت اطلاعات، شبکه، امنیت شبکه و امنیت سایبری در تاریخ ۲۱ بهمن ۱۳۹۹ توسط مرکز تخصصی آپا دانشگاه رازی با شرکت دانشجویان و علاقمندان برای ورود به حوزه‌های مذکور برگزار گردید. همچنین در پایان این رویداد به کلیه سوالات شرکت‌کنندگان پرداخته شد.

اخبار کوتاه

رفع باگ عجیب ویندوز ۱۰ توسط مایکروسافت

ویندوز۱۰ دارای یک باگ مخرب است که می تواند به هارد دیسک شما آسیب وارد کند.

اکنون شرکت مایکروسافت در تلاش است تا این باگ را برطرف کند. محقق امنیتی Jonas L این باگ را در ویندوز ۱۰ کشف کرده است و گفت: این باگ می‌تواند در یک فایل ZIP یا پوشه یا میانبر ویندوز پنهان شود. بنابراین، اگر پوشه آلوده یا فایل ZIP باز شود، باگ فعال شده و هارد دیسک را خراب می کند. این باگ در ویندوز ۱۰ به مدت سه سال وجود داشته است.

ویل دورمن تحلیلگر آسیب پذیری، این موضوع را تأیید کرد. وی همچنین فاش کرده است که این باگ در سه سال گذشته در ویندوز ۱۰ وجود داشته است. او همچنین دو سال پیش یک مورد دیگر از NTFS را گزارش کرده است که هنوز برطرف نشده است.

سخنگوی مایکروسافت گفت: "ما از این موضوع مطلع هستیم و در نسخه آینده با بروزرسانی این مشکل را حل خواهیم کرد. ما به مشتریان خود توصیه می کنیم هنگام باز کردن پرونده های ناشناخته نکات امنیتی را رعایت نمایند."

ویل دورمن نشان داده است که این باگ می تواند در بسیاری موارد با باز کردن حتی یک فایل HTML، و یا یک کپی پیست ساده در نوار آدرس مرورگر فعال شود. مایکروسافت نیز این موضوع را تأیید کرده و گفته است که در تلاش است تا آن را برطرف کند.

طبق آخرین گزارش ها، از تمام کاربران ویندوز ۱۰ که به وسیله این باگ آسیب دیده‌اند، خواسته می شود رایانه های خود را مجدداً بروزرسانی کرده و هارد دیسک خراب را تعمیر کنند. با این حال، ممکن است این باگ برای همه کاربران فعال نشود.

سرقت اطلاعات با بروزرسانی اپلیکیشن شاد

پیام‌های جعلی که در فضای مجازی به دانش‌آموزان در راستای بروز رسانی اپلیکشین شاد ارسال می شود فریبی برای به سرقت رفتن اطلاعات گوشی دانش‌آموزان است.

اخیراً شاهد ارسال پیامک‌هایی با عنوان "به روز رسانی اپلیکیشن شاد" از سوی هکرها به دانش‌آموزان هستیم، در این پیام‌ها از دانش‌آموزان خواسته شده تا اپلیکیشن شاد خود را به روز کرده در غیر این صورت اپلیکیشن شاد آن‌ها غیر فعال شده و دیگر خدماتی به آن‌ها ارائه نمی‌دهد. پیام‌هایی که از سوی مجرمان سایبری برای دانش‌آموزان از طریق فضای مجازی ارسال می‌شوند هدف آن‌ها چیزی جزء سرقت اطلاعات گوشی نمی‌باشد. دانش‌آموزان و خانواده‌های آن‌ها، اصلا به این پیام‌ها توجه نکرده و به لینک‌های ارائه شده در این پیام‌ها مراجعه نکنند چرا که احتمال سرقت اطلاعات شخصی آن‌ها وجود دارد.

دوره‌های آنلاین مرکز آپا دانشگاه رازی

★ همراه با ارائه مدرک معتبر افتا ★

★ با اساتیدی مجرب ★

۲۵% تخفیف ویژه دانشجویان

همراه با تخفیف پلکانی برای دانش‌پذیران دوره‌های آپا

با همکاری انجمن علمی مهندسی کامپیوتر

دوره آموزشی پیکربندی شبکه CCNA (New)

مدرس
مهندس آرزو حسنی

یک‌شنبه‌ها
ساعت ۱۷:۳۰ الی ۲۰

مدت دوره
۶۰ ساعت

CISCO CERTIFIED CCNA ROUTING & SWITCHING

دوره آموزشی هکر قانونمند CEH v10

مدرس
مهندس شهاب ارکان

چهارشنبه‌ها
ساعت ۱۷:۳۰ الی ۲۰

مدت دوره
۴۵ ساعت

CEH v10 Certified Ethical Hacker

دوره آموزشی مقدماتی امنیت شبکه Security+

مدرس
مهندس مهدی فرهمند

روزهای ۲۳، ۲۴ و ۳۰
بهمن، و ۱ اسفند

مدت دوره
۳۲ ساعت

CompTIA Security+

مهلت ثبت‌نام تا ۸ اسفند ماه ۱۳۹۹

جهت ثبت‌نام به آدرس evand.com/events/apa-razii مراجعه نمایید.

دوره‌ها مطابق با سرفصل‌های استاندارد تدریس می‌شوند.

APARazi APA_Razi ۰۸۳۳۴۳۴۳۲۵۱


٪۲۰ تخفیف دانشجویی
ثبت‌نام دوره‌های
مرکز آپا دانشگاه رازی
همراه با ارائه گواهی معتبر دارای اعتبار افتا
با اساتید مجرب دارای مدارک بین المللی
آنلاین
دوره امنیت شبکه سیسکو CCNA Security
۴۰ ساعت
یکشنبه‌ها
ساعت ۱۷ الی ۲۰
مهندس شهاب ارکان
CISCO CERTIFIED CCNA SECURITY
حضوری
دوره حرفه‌ای شبکه CCNP Enterprise
(New)
۶۰ ساعت
شنبه‌ها
ساعت ۱۷ الی ۲۰
مهندس سعید زنگنه
CISCO CERTIFIED CCNP ENTERPRISE
حضوری
دوره پیکربندی و مدیریت ویندوز سرور ۲۰۱۹
۶۰ ساعت
سه‌شنبه‌ها
ساعت ۱۷ الی ۲۰
مهندس محمد عزیزی
MICROSOFT CERTIFIED PROFESSIONAL Microsoft MCSA Windows Server 2016
با همکاری انجمن علمی مهندسی کامپیوتر
جهت ثبت‌نام به آدرس evand.com/events/raziapa-99 مراجعه نمایید.
cert.razi.ac.ir
APA_Razi
APARazi
۰۸۳۳۴۳۴۳۲۵۱

مرکز تخصصی آپا دانشگاه رازی