بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره سی‌ام

تیرماه ۱۴۰۰

فایرفاکس

و آسیب‌پذیری‌هایی که می‌تواند آن را طعمه‌ی هکرها سازد

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:

مرکز تخصصی آپا دانشگاه رازی

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

همکاران این شماره:

سهیلا مرادی

پویا شکری

سیده آرزو حسنی

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

آسیب‌پذیری‌های بحرانی در افزونه File Management وردپرس

نقص‌های خطرناکی در افزونه File Management وردپرس کشف شده است که امکان اجرای حملات مختلفی مانند حذف صفحات سایت و اجرای کد از راه دور را بر روی وب‌سایت فراهم می‌کند.

این افزونه به گونه‌ای طراحی شده است که با استفاده از آن مدیران سایت می‌توانند فایل‌های وب‌سایت خود را به صورت کاملاً حرفه‌ای مدیریت کنند. این افزونه با وجود امکانات بسیار متنوع خود به مدیر این امکان را می‌دهد تا بتواند با این سطوح دسترسی، از دسترسی کاربران مشخص به فایل‌ها بهره‌مند شده و برای هر کاربر به صورت جداگانه پوشه جدید جهت ذخیره فایل راه‌اندازی کند.

مدیر می‌تواند دسترسی‌های مختلفی مانند خواندن و یا نوشتن را در اختیار کاربران قرار دهد.

یکی از این نقص‌ها آسیب‌پذیری cross-site scripting (XSS) است که وب‌سایت‌های دارای پلاگین Frontend File Manager را تحت تأثیر قرار داده و به کاربران احراز هویت نشده اجازه می‌دهد کدهای جاوااسکریپت مخرب خود را به منظور ایجاد حساب‌های کاربری ادمین بر روی سایت آسیب‌پذیر تزریق نمایند.

این نقص یکی از ۶ آسیب‌پذیری بحرانی است که نسخه ۱۷.۱ و ۱۸.۲ پلاگین Front File Manager وردپرس را که در بیش از ۲۰۰۰ سایت وردپرسی فعال است تحت تأثیر قرار می‌دهد. وردپرس برای هر ۶ آسیب‌پذیری که در روز دوشنبه به صورت عمومی منتشر شدند وصله‌های امنیتی منتشر نموده است.

محققان Ninja Technologies Network اظهار داشتند این آسیب‌پذیری‌ها راه را برای طیف وسیعی از حملات اجرای کد از راه دور که هکرها را قادر به تغییر یا حذف پست‌ها، تقویت اسپم‌ها، امکان ارتقاء سطح دسترسی و انجام حملات stored cross-site scripting (XSS) بر روی سایت‌های وردپرسی می‌سازد باز می‌کنند. شرح این ۶ آسیب‌پذیری در زیر آورده شده است:

آسیب‌پذیری Stored XSS

به گفته‌ی محققان، نقص XSS امکان تزریق محتوای غیرمجاز به وب‌سایت را فراهم می‌کند.

"wpfm_edit_file_title_desc" AJAX action یک تابع " wpfm_edit_file_title_desc" را بارگیری می‌کند که هنگام ویرایش پست‌های سایت مورد استفاده قرار می‌گیرد. این تابع فاقد امنیت است، چرا که تأیید نمی‌کند آیا کاربران در حال ویرایش پست‌های خود هستند یا خیر. بنابراین، یک کاربر احراز هویت نشده می‌تواند محتوا و عنوان هر صفحه و هر پستی از سایت را به دلخواه خود تغییر دهد. علاه بر آن، اگر پست از نوع wpfm-files باشد، امکان تزریق کد جاوااسکریپت در title پست وجود دارد، چرا که این افزونه برای sanitize متغیر [‘file_title’]$_REQUEST فقط به تابع esc_attr متکی است که در آن خروجی attributeهای HTML در بک‌اند نشان داده خواهد شد و زمانی که کاربر مدیر از صفحه‌ی تنظیمات افزونه بازدید می‌کند کد جاوااسکریپت اجرا می‌شود. بنابراین، یک کاربر احراز هویت نشده می‌تواند به منظور ایجاد یک حساب کاربری ادمین کد جاوااسکریپت دلخواه خود را تزریق نماید.

ارتقاء سطح دسترسی

این نقص، از عملکرد تابع "wpfm_get_current_user" ناشی می‌شود. این تابع برای بازیابی شناسه کاربر از اسکریپت "nmedia-user-file-uploader/inc/helpers.php" مورداستفاده قرارمی‌گیرد. محققان تشریح کردند:"اگر کاربر احراز هویت شده باشد شناسه‌ی کاربر از تابع get_current_user_id در وردپرس، و اگر لاگین نکرده باشد از گزینه wpfm_guest_user_id در افزونه بازگردانده می‌شود." این بدان معناست که کاربر چه احراز هویت شده باشد چه نشده باشد می‌تواند هر شناسه‌ای را به متغیر [‘file_owner’]$_GET اختصاص دهد تا L318 $current_user_id را نادیده بگیرد و از این طریق ارتقاء سطح دسترسی را منجر شود.

تغییر تنظیمات و بارگذاری فایل‌های دلخواه

آسیب‌پذیری دیگر به کاربر احراز هویت شده اجازه می‌دهد تنظیمات افزونه را تغییر دهد. تابع "wpfm_save_settings" از اسکریپت "nmedia-user-file-upload-er/inc/admin.php"، توسط wpfm_save_settings AJAX action بارگیری می‌شود و برای ذخیره‌ی تنظیمات افزونه مورد استفاده قرار می‌گیرد که هیچ قابلیت امنیتی برای آن در نظر گرفته نشده است. بنابراین، مهاجم می‌تواند با اضافه کردن PHP به لیست نوع‌فایل‌های مجاز، از این آسیب‌پذیری بهره‌برداری نماید.

تجزیه و تحلیل‌ها نشان می‌دهد با استفاده از "wpfm_upload_file" AJAX action، مهاجم می‌تواند یک اسکریپت PHP بارگذاری کند که به صورت "http://example.com/wp-content/uploads/user_uploads/<us-ername>/<file>.php" در دسترس باشد و منجر به اجرای کد از راه دور شود.

حذف پست

آسیب‌پذیری چهارم به یک مهاجم احراز هویت نشده اجازه می‌دهد هر صفحه و پستی را از سایت حذف کند.

"wpfm_delete_file" AJAX action به صورت غیرمجاز تابع "wpfm_delete_file" را از اسکریپت "nmedia-user-file-uploader/inc/-files.php" بارگیری می‌کند، یک شناسه [‘file_id’]$_REQUEST می‌گیرد و پست مربوطه را حذف می‌کند. مشکل اینجاست که این افزونه تأیید نمی‌کند که آیا کاربر مجاز است پست را حذف کند یا خیر و از این جهت فاقد امنیت لازم است.

تغییر غیرمجاز متادیتای پست و دانلود فایل‌های دلخواه مهاجمان همچنین می‌توانند متادیتای پست‌ها را به دلخواه خود تغییر دهند که می‌تواند منجر به دانلود فایل‌های دلخواه شود. wpfm_file_meta_update’AJAX action تابع " wpfm_file_meta_update" را به صورت غیرمجاز از اسکریپت "nmed-ia-user-file-uploader/inc/files.php" بارگیری می‌کند و برای تغییر متادیتای پست‌ها مورد استفاده قرا ر می‌گیرد. داده‌ها اعتبارسنجی یا Sanitize نمی‌شوند و هیچ اقدام امنیتی برای آن در نظر گرفته نشده است.

طبق تجزیه و تحلیل‌های صورت گرفته، مهاجمان با اختصاص دادن "wpfm_dir_path" به "$meta_key" و "wp-config.php" برای "$meta_value" می‌توانند از این حفره امنیتی برای تغییر متادیتای پست‌ها سوءاستفاده کنند و سپس به جای فایل بارگذاری شده، اسکریپت "w5p-config.php" را دانلود کنند.

تزریق HTML غیرمجاز

آخرین آسیب‌پذیری به کاربر احراز هویت نشده اجازه می‌دهد از وب‌سایت به عنوان spam relay استفاده کند. این نقص از تابع " wpfm_send_file_in_email" در اسکریپت "nmedia-user-file-uploader/inc/callback-functions.php" ناشی می‌شود و برای کاربر امکان ارسال ایمیل را فراهم می‌کند.

از آنجا که ایمیل‌ها در فرمت HTML ارسال می‌شوند و مورد بررسی قرار نمی‌گیرند، می‌توان کد HTML (در قالب متن، تصویر، CSS و غیره) در آن‌ها تزریق کرد تا ایمیل به طور کامل سفارشی شود. علاوه بر این، حتی اگر [‘file_id’]$_REQUEST خالی یا نامعتبر باشد، پیام به هر حال ارسال می‌شود.

توصیه امنیتی

کاربران به منظور محافظت از خود در برابر این حملات، باید افزونه‌ی خود را به نسخه‌ی ۱۸.۳ یا بالاتر ارتقاء دهند.

منبع خبر :

Scan Link

۳۰ میلیون از دستگاه‌های شرکت Dell در معرض خطر حملات BIOS از راه دور (RCE)

چهار مسئله امنیتی مهم که به دلیل مکانیزم به‌روزرسانی معیوب دستگاه‌های DELL ایجاد شده‌اند، موجب کنترل و ماندگاری تقریباً کامل مهاجم بر روی سیستم‌های هدف می‌شوند.

محققان امنیتی بیان کردند: چهار آسیب‌پذیری با شدت بالا که می‌تواند به مهاجمان از راه دور امکان اجرای کد دلخواه در سیستم هدف، قبل از بوت شدن سیستم‌عامل در دستگاه های Dell را بدهد، کشف شده است. آن‌ها تخمین می زنند که ۳۰ میلیون دستگاه Dell در سراسر جهان وجود دارد که در معرض این آسیب‌پذیری‌ها قرار دارند.

مطابق تجزیه و تحلیل‌های تیم امنیتی Eclypsium، این آسیب‌پذیری‌ها بر روی ۱۲۹ مدل لپ‌تاپ، تبلت و کامپیوتر، از جمله دستگاه‌های سازمانی و شخصی، که توسط Secure Boot محافظت می‌شوند، تأثیر می‌گذارد. Secure Boot یک استاندارد امنیتی است که هدف آن اطمینان از آن است که یک دستگاه فقط با استفاده از نرم‌افزاری که مورد اعتماد سازنده تجهیزات اصلی دستگاه (OEM) است، عمل می‌کند تا از نفوذ غیرمجاز در سیستم جلوگیری کند.

محققان Eclypsium روز پنجشنبه بیان کردند که این آسیب‌پذیری‌ها، به مهاجمان در یک شبکه اجازه می‌دهد تا بتوانند روند حفاظتی Secure Boot را دور بزنند، روند راه اندازی دستگاه را کنترل کنند و سیستم عامل و کنترل‌های امنیتی لایه بالاتر را کنار بزنند. شدت این آسیب‌پذیری‌ها ۸.۳ از ۱۰ می‌باشد.

به طور خاص، این آسیب‌پذیری‌ها بر قابلیت BIOSConnect در Dell SupportAs-sist (یک راه‌حل پشتیبانی فنی که روی اکثر دستگاه‌های Dell مبتنی بر ویندوز نصب) تأثیر می‌گذارند. BIOSConnect برای انجام عملیات ریکاوری سیستم عامل از راه دور یا بروزرسانی سیستم عامل استفاده می‌شود.

محققان در تحلیل خود خاطرنشان کردند: "فروشندگان فناوری‌های مختلف، به طور فزاینده‌ای فرآیندهای به‌روزرسانی را انجام می‌دهند تا به کاربران خود کمک کنند که سیستم‌عامل خود را به‌روز نگه دارند و یا بازیابی کنند. گرچه این قابلیت یک ویژگی ارزشمند است، اما هرگونه آسیب‌پذیری در این فرآیندها ، مانند مواردی که در BIOSConnect Dell مشاهده کرده‌ایم، می‌تواند عواقب جدی داشته باشد."

همچنین در این گزارش اشاره شده است که این آسیب‌پذیری‌های خاص، به مهاجم اجازه می‌دهد تا از راه دور از سیستم‌عامل میزبان سوءاستفاده کرده و کنترل دستگاه را در دست بگیرد.

در پایان این گزارش آمده است: " قابلیت بهره برداری از راه دور و دستیابی به سطح دسترسی بالا احتمالاً عملکرد به‌روزرسانی از راه دور را در آینده به یک هدف جذاب برای مهاجمان تبدیل خواهد کرد."

اتصال TLS ناامن: جعل هویت Dell

اولین آسیب‌پذیری (CVE-2021-21571) ابتدای زنجیره‌ای است که می‌تواند منجر به اجرای کد از راه دور شود.

وقتی BIOSConnect تلاش می‌کند برای انجام به‌روزرسانی یا ریکاوری از راه دور، به سرور Dell HTTP متصل شود، این امکان را به BIOS سیستم می‌دهد که با سرویس Dell backend از طریق اینترنت ارتباط برقرار کند. سپس، فرآیند به‌روزرسانی یا ریکاوری را هماهنگ می‌کند.

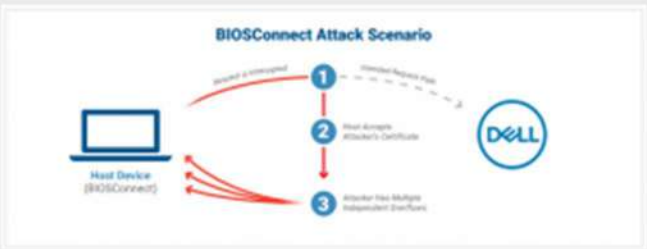
مسئله این است که اتصال TLS که برای اتصال BIOS به سرورهای backend استفاده می‌شود ، هرگونه گواهی wildcard معتبر را می‌پذیرد، محققان Eclypsium بیان کردند: "بنابراین، مهاجم با موقعیت دسترسی به شبکه میزبان، می‌تواند اتصال را رهگیری کند، هویت Dell را جعل کند و محتوای کنترل شده توسط خود را به دستگاه قربانی تحویل دهد."

بر اساس تجزیه و تحلیل‌ها، روند تأیید گواهی برای dell.com با بازیابی رکورد DNS از سرور رمزگذاری شده ۸.۸.۸.۸ بوده و سپس اتصال [به سایت بارگیری Dell] انجام می‌شود. با این حال، هرگونه گواهی wildcard معتبر صادر شده توسط هر یک از موارد تأیید شده داخلی گواهی موجود در قابلیت BIOSConnect در BIOS، شرایط اتصال ایمن را برآورده می‌کند و BIOSConnect برای بازیابی فایل‌های مربوطه اقدام می‌کند.

امکان اجرای خودسرانه کدها با سوءاستفاده از آسیب‌پذیری‌های سرریز

مهاجمان در ابتدا از آسیب‌پذیری "gatekeeper" برای انتقال محتوای مخرب به دستگاه قربانی سوءاستفاده می‌کنند، سپس یکی از سه آسیب‌پذیری متمایز سرریز (CVE-2021-21574 ، CVE-2021-21573 ، CVE-2021-21572) را انتخاب می‌کنند که هر کدام از آن‌ها می‌تواند به منظور RCE قبل از بوت شدن دستگاه هدف، مورد استفاده قرار گیرد. به گفته Eclypsium، دو مورد از این آسیب‌پذیری‌ها بر روند ریکاوری سیستم‌عامل تأثیر می‌گذارند، در حالی که مورد سوم بر روند به‌روزرسانی سیستم‌عامل تأثیر می‌گذارد. هنوز جزئیات فنی بیشتری در این خصوص منتشر نشده است.

محققان بیان کردند:" هر سناریوی حمله به یک مهاجم نیاز دارد تا بتواند ترافیک شبکه قربانی را دنبال و هدایت کند، مانند حمله مرد میانی (MITM) که مانع چندانی نیز برای حمله ندارد."



حملات مرد میانی حملاتی با پیچیدگی نسبتاً کم برای مهاجمان است و با تکنیک‌هایی مانند ARP spoofing و DNS cache poisoning انجام می‌شود.

علاوه بر این، VPN های سازمانی و دستگاه‌های شبکه در یک سازمان به هدف اصلی مهاجمان تبدیل شده‌اند و نقص در این دستگاه‌ها می‌تواند به مهاجمان اجازه هدایت ترافیک شبکه را بدهد. در نهایت، کاربران نهایی که از خانه کار می‌کنند و به طور فزاینده‌ای به شبکه SOHO متکی هستند، در معرض این آسیب‌ها قرار می‌گیرند.

آسیب‌پذیری در این نوع دستگاه‌های شبکه کاملاً رایج بوده و در کمپین‌های تهاجمی گسترده‌ای مورد بهره برداری قرار گرفته است.

با توجه به اینکه بهره‌برداری موفقیت آمیز BIOS یک دستگاه به مهاجمین اجازه می‌دهد که با بالاترین سطح دسترسی روی دستگاه کنترل داشته باشند و ماندگاری مداوم ایجاد کنند، تلاش‌های اساسی در این راستا، احتمالاً یک گام مثبت برای مهاجمان سایبری محسوب می‌شود. آن‌ها همچنین می‌توانند روند بارگیری در سیستم‌عامل میزبان را کنترل کنند و لایه‌های امنیتی و حفاظتی را غیرفعال کرده تا شناسایی نشوند.

محققان Eclypsium همچنین بیان کردند: "کنترل تقریباً نامحدودی که بر روی دستگاهی که این حمله بر روی آن اتفاق میافتد فراهم می‌شود، ثمره‌ای بسیار ارزشمند برای مهاجمان ایجاد می‌کند.

توصیه امنیتی

Dell وصله‌های منتشر شده در خصوص آسیب‌پذیری BIOS را بر روی تمام سیستم های آسیب دیده به صورت خودکار نصب کرده است. برای مشاهده جزئیات بیشتر، به قسمت مشاوره وبسایت آن مراجعه کنید.

Eclypsium در ادامه به کاربران توصیه می‌کند: "پس از بررسی دستی هش‌ها در موارد منتشر شده توسط Dell، از خود سیستم عامل فرآیند بروزرسانی BIOS را اجرا کنید."

منبع خبر :

Scan Link

اخبار کوتاه

ایجاد حفره‌های امنیتی با تنظیمات نادرست در اکثر محیط‌های Active Directory

پیکربندی‌های اشتباه در سرویس‌های صدور گواهینامه Active Directory می‌تواند به مهاجمان اجازه سرقت اطلاعات را بدهد.

Lee Christensen و Will Schroeder معماران فنی در SpecterOps، گفتند: "طبق تجربه ما، تقریباً درهر نصب Active Directory که در یک دهه گذشته بررسی کرده‌ایم، هرکدام نوعی مشکل در پیکربندی داشته‌اند."

سرویس گواهی Active Directory (AD CS) یکی از مؤلفه‌های اصلی زیرساخت کلید عمومی مایکروسافت (PKI) است که برای مدیریت گواهینامه‌های مورداستفاده در توابعی مانند رمزگذاری، امضای پیام و احراز هویت، با سایر خدمات AD، ازجمله Domain Services و Certificate Authority، هماهنگ است.

Lee Christensen و Will Schroeder در مقاله خود بیان کردند چندین تنظیم غلط در AD CS می‌تواند منجر به سوءاستفاده در زمینه‌های زیر شود:

- سرقت اعتبارنامه با سوءاستفاده از ثبت‌نام کاربران و رایانه‌ها در گواهینامه‌ها و سرقت گواهینامه‌های موجود. به گفته محققان اگر طرح سرقت اعتبارنامه از تغییرات رمز عبور جان سالم به دربرد و می‌تواند احراز هویت هوشمند را دور بزند.
- روش‌های افزایش امتیاز که به مهاجمان اجازه می‌دهد تا به کاربر مطرح در دامنه تبدیل شوند.
- حملات پایداری دامنه که به مهاجمان اجازه می‌دهد مانند هر کاربر Active Directory وارد سیستم شوند.

محققان هشدار دادند، با توجه به کنترل گسترده AD بر منابع سازمان‌ها، سوءاستفاده از این آسیب‌پذیری‌ها به مهاجمان اجازه می‌دهد تا به صندوق‌های پستی دسترسی داشته باشند، سال‌ها در شبکه‌های در معرض خطر باقی بمانند، بدافزار را از طریق خط مشی‌های به‌روزرسانی و در سطح دامنه توزیع کنند و داده‌های حساس را به خطر بیندازند.

محققان گفتند: این حفره‌ها به‌احتمال‌زیاد نتایج حاصل از تنظیمات اشتباه و بدون درک از پیامدهای امنیتی توسط مدیران سیستم و مدیران IT است.

تقریبا نیمی از قربانیان باج‌افزار مجدداً توسط همان مهاجم مورد حمله قرار می گیرند!

بر اساس آمار، نزدیک به ۴۶ درصد از قربانیان باج‌افزار دوباره توسط همان هکرهای قبلی مورد حمله قرار می‌گیرند و بعضی از آن‌ها، هرگز به داده‌های مسروقه‌ی خود دست پیدا نمی‌کنند.

تحقیقاتی توسط Censuswide صورت گرفته است که نشان می‌دهد ۸۰ درصد از سازمان‌هایی که پس از حمله هکرها مجبور به پرداخت باج شده‌اند، پس از مدتی بار دیگر مورد حمله قرار گرفته‌اند. که نزدیک به ۴۶ درصد از حملات مجدد به سازمان‌ها توسط گروه هکرهای قبلی صورت گرفته است؛ برای مثال یکی از شرکت‌ها پس از اینکه مورد حمله توسط باج‌افزارها قرار گرفت، مجبور به پرداخت باج با رمزارز شد تا اطلاعات مهم این شرکت حفظ شود؛ اما همان هکرهایی که به این شرکت حمله کرده بودند، پس از دو هفته حمله‌ی دیگری به داده‌های سرور آن کردند.

بسیاری فکر می‌کنند پرداخت باج به هکرها بابت بازگشت اطلاعات، هزینه‌ی فراوانی برای قربانیان دارد؛ اما این گونه نیست. در واقع از دست رفتن اعتبار سازمان‌ها و شرکت ها پس از حمله‌ی سایبری، بزرگ‌ترین ضربه را به قربانیان می‌زند. ۵۳ درصد از سازمان‌ها گفته‌اند پس از حمله‌ی سایبری، تبلیغات منفی علیه آن‌ها صورت گرفته است و ۶۶ درصد از قربانیان گفته‌اند پس از حمله، مشتریان خود را از دست داده و با کاهش درآمد مواجه شده‌اند. تحلیلگران معتقد هستند که آمار حملات سایبری در سال ۲۰۲۱ نسبت به سال گذشته‌ی میلادی تقریبا دو برابر شده است و هر یک از این حملات به از دست رفتن داده‌های مهم سازمان‌ها منجر می‌شود؛ داده‌هایی که سازمان‌ها حاضر هستند میلیون‌ها دلار بابت دستیابی مجدد به آن‌ها پرداخت کنند. تخمین زده می‌شود که در سال ۲۰۳۱، باج‌گیری هکرها از قربانیان به مرز ۲۶۵ میلیارد دلار برسد.

با این تفاسیر، نباید پس از حملات باج‌افزاری، راه نفوذ آن‌ها را نادیده گرفت و به رفع و رجوع موقتی بسنده کرد، چرا که هکرها بازهم به شرکت یا سازمان شما بازمی‌گردند.

آسیب پذیری

آسیب‌پذیری در مرورگر Mozilla Firefox

چندین آسیب‌پذیری در مرورگر محبوب موزیلا فایرفاکس یافت شده است که امکان اجرای کد از راه دور را برای مهاجم فراهم می‌کند.

این آسیب‌پذیری‌ها به شرح زیر می‌باشند:

CVE-2021-29970: آسیب‌پذیری Use-after-free در accessibility قابلیت‌های یک سند

شدت: بالا

شرح آسیب‌پذیری: یک صفحه‌ی وب مخرب می‌تواند موجب نقص use-after-free، خرابی حافظه و به صورت بالقوه crash قابل بهره‌برداری شود. این آسیب‌پذیری تنها زمانی فایرفاکس را تحت تأثیر قرار می‌دهد که accessibility فعال باشد.

CVE-2021-29971: صرف‌نظر از شِما و پورت و تنها بررسی میزبان، هنگام بررسی مجوزهای اعطاء شده

شدت: بالا

شرح آسیب‌پذیری: اگر کاربر مجوزی را به یک صفحه وب داده باشد و آن مجوز را ذخیره کرده باشد، به هر صفحه وب دیگری که روی همان میزبان اجرا می‌شود – صرف نظر از شِما یا پورت – این مجوز داده می‌شود. این آسیب‌پذیری تنها فایرفاکس نسخه اندروید را تحت تأثیر قرار می‌دهد و سایر سیستم‌عامل‌ها تحت تأثیر قرار نمی‌گیرند.

CVE-2021-30547: نوشتن خارج از محدوده در ANGLE

شدت: بالا

شرح آسیب‌پذیری: این آسیب‌پذیری به مهاجم اجازه می‌دهد با خراب کردن حافظه منجر به crash قابل بهره‌برداری شود.

CVE-2021-29972: استفاده از کتابخانه منسوخ شده حاوی آسیب‌پذیری use-after-free

شدت: متوسط

شرح آسیب‌پذیری: این آسیب‌پذیری از طریق تست و در کتابخانه منسوخ شده Cairo یافت شد. به‌روزرسانی کتابخانه این مسئله را برطرف نموده است و ممکن است آسیب پذیری‌های امنیتی ناشناخته دیگر را نیز برطرف کند.

CVE-2021-29973: فعال شدن تکمیل خودکار گذرواژه در وب‌سایت‌های HTTP بدون تعامل کاربر در Android

شدت: متوسط

شرح آسیب‌پذیری: در این آسیب‌پذیری، تکمیل خودکار گذرواژه بدون تعامل کاربر در وب‌سایت‌های ناامن در Firefox برای Android فعال می‌شود. قبل از اینکه گذرواژه کاربر با قابلیت تکمیل خودکار مرورگر وارد شود، می‌بایست مستلزم تعامل کاربر با صفحه باشد. این نقص تنها Firefox نسخه Android را تحت تأثیر قرار می‌دهد و سایر سیستم‌عامل‌ها تحت تأثیر قرار نمی‌گیرند.

CVE-2021-29974:نادیده گرفته شدن خطاهای HSTS هنگام فعال بودن پارتیشن‌بندی شبکه

شدت: متوسط

شرح آسیب‌پذیری: هنگامی که پارتیشن‌بندی شبکه فعال باشد، یعنی به عنوان مثال، در نتیجه تنظیمات Enhanced Tracking Protection، یک صفحه خطای TLS به کاربر اجازه می‌دهد خطایی را در دامنه که نشان‌دهنده‌ی HTTP Strict Transport Security است نادیده بگیرد (بدان معنا که خطا نباید قابل چشم‌پوشی باشد). این نقص تأثیری در ارتباطات شبکه ندارد و آن‌ها به طور خودکار به HTTPS ارتقاء داده می‌شوند.

CVE-2021-29975: امکان قرار دادن پیام متنی در بالای یک وب‌سایت دیگر

شدت: متوسط

شرح آسیب‌پذیری: به واسطه‌ی برخی دستکاری‌ها در DOM، پیامی که تحت کنترل مهاجم است اما در قالب HTML یا فرمت‌های دیگر نیست می‌تواند در بالای یک دامنه دیگر (با یک دامنه جدید که در نوار آدرس نشان داده می‌شود) قرار گیرد که در نهایت سردرگمی کاربر را منجر شود.

CVE-2021-29976: رفع ایرادات امنیتی حافظه در FireFox 90 و Firefox ESR 78.12

شدت: بالا

شرح آسیب‌پذیری: توسعه‌دهندگان موزیلا Emil Ghitta، Tyson Smith، Valen-tin Gosu، Olli Pettay و Randell Jesup از وجود آسیب‌پذیری‌های امنیتیِ حافظه در Firefox 89 و Firefox ESR 78.11 خبر دادند. برخی از این نقص‌ها شواهدی از خرابی حافظه را نشان می‌دهند و تصور ما این است که با تلاش کافی می‌توان برای اجرای کد دلخواه از این آسیب‌پذیری‌ها بهره‌برداری کرد.

CVE-2021-29977: رفع نقص‌های امنیتی حافظه در Firefox 90

شدت: بالا

شرح آسیب‌پذیری: Andrew McCreight، Tyson Smith، Christian Holler و Gabriele Svelto، توسعه‌دهندگان موزیلا از وجود آسیب‌پذیری‌های امنیتیِ حافظه در Firefox 89 خبر دادند. برخی از این نقص‌ها شواهدی از خرابی حافظه را نشان می‌دهند و تصور ما این است که با تلاش کافی می‌توان برای اجرای کد دلخواه از این آسیب‌پذیری‌ها بهره‌برداری کرد.

CVE-2021-29977: رفع نقص‌های امنیتی حافظه در Firefox 90

شدت: بالا

شرح آسیب‌پذیری: Andrew McCreight، Tyson Smith، Christian Holler و Gabriele Svelto، توسعه‌دهندگان موزیلا از وجود آسیب‌پذیری‌های امنیتیِ حافظه در Firefox 89 خبر دادند. برخی از این نقص‌ها شواهدی از خرابی حافظه را نشان می‌دهند و تصور ما این است که با تلاش کافی می‌توان برای اجرای کد دلخواه از این آسیب‌پذیری‌ها بهره‌برداری کرد.

توصیه امنیتی:

آسیب‌پذیری‌های مذکور در Firefox 90 برطرف شده‌اند، به کاربران توصیه می‌شود در اسرع وقت مرورگر فایرفاکس خود را به‌روزرسانی نمایند.

منبع خبر :

Scan Link

رفع آسیب‌پذیری روز صفر با شدت بحرانی در برخی محصولات SolarWinds

آسیب‌پذیری روز صفرم با شناسه CVE-2021-35211 در محصولات Serv-U به مهاجم این امکان را خواهد داد تا از راه دور کد دلخواه خود را اجرا کرده (RCE) و از این آسیب‌پذیری بهره‌برداری کند.

این نقص امنیتی بر روی سرورهایی که SSH آن‌ها فعال باشد و همچنین محصولات Serv-U Manage File Transfer Server و Serv-U Secured FTP تأثیر خواهد گذاشت. SolarWinds از طریق شرکت مایکروسافت از این آسیب‌پذیری مطلع شد.

آسیب‌پذیری مذکور دارای شدت بحرانی بوده که در نسخه‌ی Serv-U 15.2.3 HF1 و قبل‌تر وجود دارد و با انتشار وصله‌ی امنیتی hotfix (HF) 2 15.2.3 این نقص رفع شده است. گفتنی است که سایر محصولات SolarWinds و N-able (یا همان SolarWinds MSP) از جمله پلتفرم Orion و تمامی ماژول‌های آن، تحت تأثیر این آسیب پذیری قرار نمی‌گیرند.

مهاجم در صورت بهره‌برداری موفق از این نقص امنیتی می‌تواند در Serv-U سیستم

میزبان به امتیاز دسترسی بالایی برسد. شرکت SolarWinds هنوز براوردی از تعداد مشتریانی که تحت تأثیر این آسیب‌پذیری قرار گرفته‌اند ارائه نداده است. کارشناسان امنیتی خاطر نشان کردند که این مسئله ارتباطی به حمله زنجیره‌ای SolarWinds ندارد و این شرکت برخی از شاخص‌های تشخیص (IOCs) را منتشر کرد ولی هنوز اطلاعات دقیق و جزئیات فنی این آسیب‌پذیری را فاش نکرده است. شرکت SolarWinds از کاربران خواست تا هر چه سریع‌تر نسبت به نصب بروزرسانی‌های منتشر شده و رفع این نقص امنیتی مهم اقدام کنند.

توصیه امنیتی

به‌روزرسانی‌ها و وصله‌های منتشر شده برای این آسیب‌پذیری در جدول زیر آورده شده است:

محصول تحت تأثیر	روش کاهش/رفع
Serv-U نسخه 15.2.3 HF1	ارتقاء به نسخه‌ی 15.2.3 HF2 از طریق مراجعه به بخش Customer Portal سایت solarwinds
Serv-U نسخه 15.2.3	ارتقاء به نسخه‌ی 15.2.3 HF1 و سپس اعمال وصله‌ی 15.2.3 HF2 Serv-U از طریق مراجعه به بخش Customer Portal سایت solarwinds
Serv-U تمامی نسخه‌های قبل از 15.2.3	ارتقاء به نسخه‌ی 15.2.3 و اعمال وصله‌ی 15.2.3 HF1 Serv-U و سپس اعمال وصله‌ی 15.2.3 HF2 Serv-U از طریق مراجعه به بخش Customer Portal سایت solarwinds

منبع خبر :

Scan Link

آسیب‌پذیری‌های موجود در مجموعه تراشه‌های NVIDIA Jetson راه‌گشای حملات DoS و سرقت داده

این شرکت سازنده‌ی تراشه، نُه آسیب‌پذیری با شدت بالا که به نحوه مدیریت الگوریتم‌های رمزنگاری سطح پایین مرتبط است، در فریمورک Jetson SoC خود وصله کرده است.

نقص امنیتی در میلیون‌ها دستگاه اینترنت اشیا (IoT) که از تراشه‌های Jetson NVIDIA استفاده می‌کنند، راه را برای انواع هک‌ها و حملات، از جمله حملات منع سرویس (DoS) یا سرقت داده‌ها باز می‌کند.

NVIDIA وصله‌هایی را منتشر کرده است که به نُه آسیب‌پذیری با شدت بالا و هشت نقص اضافی دیگر که با شدت کمتر هستند، رسیدگی می‌کند. این وصله‌ها مجموعه گسترده‌ای از آسیب‌پذیری‌های تراشه‌های NVIDIA را که معمولاً برای سیستم‌های محاسباتی تعبیه شده، برنامه‌های یادگیری ماشین و دستگاه‌های خودکار مانند ربات‌ها و هواپیماهای بدون سرنشین استفاده می‌شود، برطرف می‌کنند.

محصولات تحت تأثیر این آسیب‌پذیری‌ها شامل سری تراشه‌های Jetson می‌شود. AGX Xavier، Xavier NX / TX2، Jetson TX1 (از جمله Jetson TX2 NX) و Jetson Nano (از جمله Jetson Nano2GB) موجود در بسته توسعه نرم‌افزار NVIDIA JetPack، از جمله آن‌ها هستند. وصله‌ها به عنوان بخشی از بولتن امنیتی ژوئن NVIDIA، که روز جمعه منتشر شد، در دسترس عموم قرار گرفتند.

مهم‌ترین وصله منتشر شده

شدیدترین این آسیب‌پذیری‌ها که با عنوان CVE-2021-34372 شناخته می‌شود، امکان حمله سرریز بافر را توسط مهاجم در فریمورک Jetson ایجاد می‌کند. مطابق بولتن امنیتی منتشر شده NVIDIA، مهاجم برای انجام حمله نیازمند دسترسی به شبکه‌ی سیستم هدف است، اما به طور کلی سوءاستفاده از این آسیب‌پذیری چندان پیچیده نیست و مهاجم با سطح دسترسی کم نیز می‌تواند از آن سوءاستفاده کند. همچنین این گزارش بیان می‌کند که مهاجم طی حمله می‌تواند دسترسی مداوم به مؤلفه های دیگر را هدف قرار دهد و به طور هدفمند سیستم هدف را دستکاری کرده یا خراب کند.

همچنین در این بولتن امنیتی عنوان شده است که درایور Jetson در کد مربوط به تجزیه پیغام در پروتکل NVIDIA OTE، دارای یک آسیب‌پذیری است که می‌تواند منجربه خطای سرریز عدد صحیح در محاسبه اندازه تابع ()malloc شده و در نهایت، خطای سرریز بافر در پشته اتفاق بیفتد. نتیجه این امر ممکن است منجر به افشای اطلاعات، افزایش امتیازات مهاجم در سیستم و حملات انکار سرویس (DoS) شود.

(Oblivious transfer(OTE، الگوریتم‌های رمزنگاری سطح پایین هستند که توسط تراشه‌های Jetson برای پردازش پروتکل‌های تنظیمات خصوصی استفاده می‌شوند که به منظور ایمن سازی داده‌ها در هنگام پردازش تراشه بر روی داده ها استفاده می‌شوند.

سایر آسیب‌پذیری‌های با شدت بالا

سایر آسیب‌پذیری‌های با شدت بالا که توسط NVIDIA وصله شده است شامل آسیب‌پذیری‌هایی با درجه شدت بین ۷ تا ۷.۹ هستند که شامل، CVE-2021-34373، CVE-2021-34376، CVE-2021-34375، CVE-2021-34734، CVE-2021-34379، CVE-2021-34378، CVE-2021-34377 و CVE 2021 34380 می‌شوند. سوءاستفاده از شش مورد از این آسیب‌پذیری‌ها، می‌تواند به یک مهاجم محلی اجازه دهد که حمله DoS را در سیستم آغاز کند.

یکی از آسیب‌پذیری‌ها (CVE-2021-34373)، با درجه شدت ۷.۹، بر هسته لینوکس Jetson تأثیر می‌گذارد و راه را برای حمله سرریز بافر مبتنی بر heap باز می‌کند. این نوع حمله در فریمورک حافظه heap data تراشه‌ها انجام می‌پذیرد، جایی که مؤلفه‌های مختلف برای ایجاد خطا دستکاری می‌شوند.

NVIDIA همچنین در بولتن امنیتی خود بیان می‌کند: "هسته لینوکس (TLK) دارای یک آسیب‌پذیری در هسته NVIDIA TLK است که در آنجا عدم نظارت کافی بر heap data باعث خطای سرریز پشته می‌شود، که ممکن است منجر به افشای اطلاعات و منع

خدمات شود."

علاوه بر Firmware، سازنده تراشه وصله‌هایی نیز برای CVE-2021-34372 تا CVE-2021-34397 برای آدرس‌دهی نقطه پایانی نرم‌افزار در سری Jetson TX1 و TX2، سری TX2 NX وAGX Xavier ، سریNano ، Xavier NX و Nano 2GB منتشر کرده است.

NVIDIA همچنین این موضوع را بیان کرده است که:" این آسیب‌پذیری‌ها به مسائل امنیتی می‌پردازند که ممکن است منجر به افزایش سطح دسترسی مهاجم، حمله منع سرویس و افشای اطلاعات شود. برای محافظت از سیستم خود، جدیدترین پکیج‌های Debian را از مخازن APT بارگیری و نصب کنید."

منبع خبر :

Scan Link

هشدار SONICWALL در خصوص حملات باج‌افزاری بر روی تجهیزات SMA و SRA

شرکت SonicWall در خصوص حملات فعال باج‌افزار ی بر روی تجهیزات دسترسی از راه دور زیر که وصله نشده یا از ثابت‌افزار نسخه‌های x.8 که دیگر پشتیبانی نمی‌شوند (EOL)، استفاده می‌کنند، هشدار داد:

- Secure Mobile Access (SMA) 100 series
- Secure Remote Access (SRA)

حملات باج‌افزاری با بهره‌برداری از یک آسیب‌پذیری شناخته‌شده که در اوایل سال ۲۰۲۱ در نسخه‌های جدیدتر توسط SonicWall وصله شده بود، انجام می‌شود. سازمان‌هایی که از تجهیزات زیر با ثابت‌افزار نسخه‌های x.8 استفاده می‌کنند باید نسخه‌ی ثابت‌افزار را به نسخه‌های x.9 یا x.10 ارتقا داده و یا به‌طور کلی اتصال آن تجهیز را از اینترنت قطع نمایند:

- SRA 4600/1600 (EOL 2019)
  - قطع سریع اتصال تجهیز
  - ریست کردن رمزهای عبور
- SRA 4200/1200 (EOL 2016)
  - قطع سریع اتصال تجهیز
  - ریست کردن رمزهای عبور
- SMA 400/200 (این تجهیز همچنان در حالت Retirement به صورت محدود پشتیبانی می‌شود)
  - به‌روزرسانی سریع به 10.2.0.7-34 یا 9.0.0.10
  - ریست کردن رمزهای عبور
  - فعال نمودن احراز هویت چند عاملی (MFA)

منبع خبر :

Scan Link

اخبار کوتاه

٦ مخـــزن رســـمی پایتـــون با بـــدافزار رمزنگاری‌شده دست به‌گریبان شد

محققان شرکت امنیتی Sonatype شش بسته مخرب تایپ کردن را در مخزن PyPI زبان برنامه‌نویسی رسمی Python کشف کرده‌اند که دارای بدافزار مخرب است.

Sonatype خدمات اتوماسیون زنجیره تأمین نرم‌افزار را ارائه می‌دهد. این شش بسته بیش از ۵۰۰۰ بار بارگیری شده است. محققان امنیتی Sonatype در گزارش خود نوشتند: "ابزار تجزیه‌وتحلیل ما به‌طور مداوم اجزای نرم‌افزار تقلبی و مخرب را قبل از حمله به زنجیره‌های تأمین نرم‌افزار مدرن ، کشف و مسدود می‌کند."

محققان Sonatype خاطرنشان کردند که بسته‌های جعلی توسط یك نویسنده با استفاده از شناسه "nedog123" ارسال‌شده است و قدمت برخی از آن‌ها تا آوریل ۲۰۲۱ است. این بسته‌ها حاوی دستورالعمل‌هایی در پرونده‌های setup.py است که بدافزارهای رمزنگاری را بارگیری و نصب می‌کند. به گفته محققان، یک بسته مخرب منفرد می‌تواند در چندین پروژه مورداستفاده قرار گیرد، دستگاه را با رمزنگارها یا سرقت اطلاعات و غیره آلوده کند ، بنابراین روند اصلاح آن بسیار دشوار است.

بسته‌های جعلی PyPI به شرح زیر است:

maratlib: ۲،۳۷۱ بارگیری

maratlib1: ۳۷۹ بارگیری

matplatlib-plus: ۹۱۳ بارگیری

mllearnlib: ۳۰۵ بارگیری

mplatlib: ۳۱۸ بارگیری

learninglib: ۶۲۶ بارگیری

بسیاری از آن‌ها Typosquats هستند ، با ۱ کاراکتر خاموش یا مشابه سایر بسته‌های یادگیری ماشین در PyPI مانند "mplatlib" به‌جای "matplotlib" اصلی. اگر از بدافزار پیشرفته‌ای استفاده کنند، ممکن است این بدافزار تأثیر نگذارد. به این دلیل که چنین بسته‌های یادگیری ماشینی معمولاً محققانی هستند که از دستگاه‌های گران‌قیمت و با عملکرد بالا لینوکس استفاده می‌کنند.

مقالات آموزشی

روش‌های ایمن‌سازی زیرساخت اکتیو دایرکتوری (بخش اول)

سرویس اکتیودایرکتوری به عنوان زیرساخت اصلی اکثر سازمان‌های سراسر جهان معرفی گردیده است که دارای ملاحظات قابل توجهی در زمینه امنیت کاربران در منابع سازمان می‌باشد. به دلیل حساسیت و اهمیت سرویس فوق، راهکارهایی به منظور ایمن‌سازی در این سرویس ارائه می‌گردد. این امر سبب می‌شود تا حد مطلوبی امنیت افزایش یابد و مانع از مشکلات احتمالی که در اثر دسترسی‌های غیرمجاز ایجاد می شوند خواهد گردید.

۱- مستند سازی موجودیت‌ها

اولین قدم در زمینه ایمن‌سازی زیرساخت اکتیودایرکتوری مستندسازی پیکربندی موجود است. اگرچه این مرحله ممکن است تا حدودی پیش پا افتاده به نظر برسد، ، اما تا زمانی که نقطه حال حاضر پروژه مشخص و شفاف نباشد، امکان حرکت به جلو موجود نخواهد بود. یکی از نقاط مناسب برای شروع این فعالیت، ساختارهای سطح بالا مانند Forest و پیکربندی دامنه‌ها، مستندسازی توپولوژی سایت‌ها مانند لیست کردن سایت‌ها می‌باشد. مستندسازی سیاست‌های دامنه (GPO) نیز از جمله مواردی است که رعایت نمودن آن بسیار ضروری بوده و در ساختار حائز اهمیت می‌باشد. این سند علاوه بر اینکه مواردی مانند سیاست‌های مرتبط به رمزعبور (Password Policies) و سیاست‌های ممیزی (Audit Policies) را ارائه می‌دهد، باید امکان بررسی اینکه سیاست‌های فوق به چه کسانی اعمال شده و کدام گروه از کاربران امکان تغییر آن را دارند را فراهم آورد. همچنین باید تمام تغییرات اعمال شده مانند تغییرات Schema به طور کامل مستندسازی شوند. علاوه بر موارد فوق باید نام کنترل‌کننده دامنه (DC)ها، نسخه سیستم‌عامل آن‌ها، نرم‌افزارهای امنیتی مانند آنتی‌ویروس، نحوه تهیه نسخه پشتیبان ذکر گردند تا در موقعیت‌های حیاتی، کمبود این اطلاعات احساس نشود.

۲- کنترل نمودن بار مدیریتی

در صورتی که به زیرساخت اکتیودایرکتوری مانند یک هرم بنگریم، امنیت در آن دقیقاً از نقاط بالایی شروع شده و برقرار می‌گردد. کنترل نمودن وظایف مدیریتی هر دامنه مهم‌ترین و شاید دشوارترین مرحله در برقراری امنیت باشد. پیشنهاد می‌گردد دسترسی‌های مدیریتی هر دامنه و گروه مدیریت آن دامنه (Domain Admins) در اختیار مدیران Forest باشد تا از بروز ناهماهنگی در ساختار جلوگیری شود. باید در نظر داشت که دسترسی مدیریتی به حتی یک کنترل کننده دامنه (DC) در دامنه‌ها ممکن است موجب

بروز ناهماهنگی گردد. در صورتی که مدیریت دامنه‌ها در اختیار گروه مجزایی قرار دارد، باید رابطه‌ای نزدیک با آن گروه ایجاد شده و قوانین و مقرراتی برای مدیریت ارائه گردد تا تمام گروه‌های مدیریتی از این مقررات یکسان تبعیت نمایند.

۳- محدود کردن تعداد کاربران Admin

در تمام مدت باید در نظر داشت که تعداد کاربران گروه Admin در ساختار کمینه گردد. اگرچه ساختار امنیتی اکتیودایرکتوری حال حاضر با ساختار گذشته خود در NT کاملاً متفاوت بوده و دارای تغییرات زیادی می‌باشد اما همچنان یک نقطه ضعف اصلی در این ساختار به چشم می‌خورد که آن عدم امکان مدیریت کامل یک کنترل‌کننده دامنه (DC) بدون نیاز به عضویت در گروه Domain Admin می‌باشد. تحت هیچ شرایطی پیشنهاد نمی‌گردد که وظایف مدیریتی خاص هر کنترل‌کننده دامنه (DC) به عهده گروه و افرادی واگذار گردد که در آینده مجبور باشیم آن‌ها را به عضویت در گروه Domain Admins در آوریم. به جای اعطای سطح دسترسی Domain Admin به اپراتورهای رایانه، راه‌حلی مناسب با ترکیبی از نرم‌افزارهای موجود در بازار و پیاده‌سازی سیاست‌های امنیتی ارائه کنید.

۴- آزمایش و تست تنظیمات Group Policy

تنظیمات و سیاست‌های دامنه (GPO) به دلیل اهمیت بالایی که در امنیت ساختار دارند باید حتماً به صورت تست پیاده سازی شوند تا از صحت عملکرد آن‌ها اطمینان حاصل شود. همچنین پیشنهاد می‌شود سیاست‌هایی که در دامنه اعمال شوند را ابتدا در OUهای خاص اعمال کرده و پس از بررسی نتایج و مثبت بودن آن، در کل دامنه اعمال گردد.

۵- استفاده از حساب‌های کاربری مجزا برای موارد مدیریتی

بعد از اینکه تعداد کاربران Administrator در ساختار کمینه گردید، باید اطمینان حاصل کرد تمام کاربرانی که فعالیتی انجام می‌دهند نیاز به سطح دسترسی بالاتری دارند، باید از حساب کاربری خاص دیگری، مجزا از حساب کاربری خود به این منظور استفاده نمایند. این حساب‌های کاربری مجزا باید از روش نامگذاری متفاوتی استفاده نموده و در OU مشخصی قرار داشته باشند تا بتوان به راحتی به آن‌ها سیاست‌های خاصی اعمال گردد. همچنین می‌توان این کاربران را گروه‌بندی کرده و با نامگذاری خاص مانند HQAccount Admins مشخص نماییم و بعد از آن گروه ذکر شده را به عضویت Account Operators در آوریم.

۶- محدود کردن عضویت در گروه‌های Built-in

سناریویی را در نظر بگیرید که یک کاربر با سطح دسترسی مدیریتی غیر مجاز (Rogue Administrator) خود را به عضویت گروه مدیران دامنه (Domain Admins) در آورد. در آن صورت قادر خواهد بود تا مقاصد خرابکانه خود را پیاده‌سازی نماید. استفاده از سیاست‌های موجود برای کنترل نمودن این امر مانند RestrictedrGroups این اطمینان را به ما می‌دهد تا کاربرانی که عضو گروه‌های حساس مانند Domain Admins و Schema Admins هستند به صورت دائم و در فاصله‌های زمانی ۵ دقیقه‌ای مجدداً بررسی می‌شوند و درصورت اضافه شدن شخص دیگری به این گروه‌ها، لیست به حالت پیش‌فرض خود بازگردد.

۷- استفاده از ترمینال سرور مجزا برای موارد مدیریتی

به دلیل دسترسی بالای کاربران مدیر به کنترل کننده دامنه (DC)ها ، توپولوژی سایت‌ها و Schema پیشنهاد می‌شود که کاربران فوق از یک سیستم مرکزی جهت اتصال به رایانه‌های Server استفاده نمایند. پیاده‌سازی این روش باعث به‌وجود آمدن یک نقطه مرکزی جهت ارتباطات می‌شود. اما نکته‌ای که باید در این روش مورد توجه قرار گیرد این است که سیستم فوق باید از لحاظ امنیتی کاملا واکسینه شده و فایل‌های به‌روزرسانی سیستم‌عامل به طور متناوب بر روی سیستم نصب شده و نرم‌افزارهای امنیتی سیستم کاملاً به‌روز باشد.

۸- غیرفعال نمودن کاربر Guest و تغییرنام کاربر Administrator

این اقدام یکی از اقدامات اصلی جهت ایمن‌سازی ساختار اکتیودایرکتوری علیه حملات هکرها می‌باشد. علاوه بر غیرفعال نمودن کاربر Guest و تغییر نام کاربر Administrator، فیلد Description آن‌ها نیز باید تغییر گردند تا نشان دهنده سطح دسترسی هر کدام از آن‌ها نباشد.

۹- محدود کردن دسترسی به کاربران Administrator

علاوه بر گروه مدیران دامنه (Domain Admins) کاربران عضو گروه مدیران محلی نیز از اهمیت بالایی برخوردار هستند. باید اطمینان حاصل نمود که رمز عبور کاربران فوق نیز در اختیار همه قرار نگیرد و تنها کاربرانی که مجاز به مدیریت سیستم‌ها هستند دارای رمز عبور باشند.

۱۰- مراقبت از رمزعبور DSRM

این رمز عبور که منحصراً به هر کدام از کنترل‌کننده‌های دامنه (DC)ها اختصاص داده می‌شود، از اهمیت ویژه‌ای در اکتیودایرکتوری برخوردار است. بهترین پیشنهاد برای ایمن‌سازی این رمز عبور راهکاری به جز تغییر متوالی این رمز عبور در فاصله‌های زمانی مشخص نیست چرا که فاش شدن این رمز عبور می‌تواند روند دستیابی به پایگاه داده اکتیودایرکتوری (NTDS.DIT) را بسیار هموار سازد.

۱۱- پیاده‌سازی سیاست‌های رمزعبور قدرتمند

اگرچه تاکنون هر کدام از ما به قابلیت‌ها و امنیت یک رمز عبور قدرتمند پی‌برده‌ایم، درک مفهوم این موضوع و مجاب کردن کاربران به استفاده از رمز عبور قدرتمند کار دشواری خواهد بود. اما با توجه به اینکه امنیت در ساختار از اهمیت بسیار بالاتری برخوردار است، باید در مجاب کردن کاربران به استفاده از رمز عبور قدرتمند و پیچیده کوشش ورزید.

۱۲- محافظت از رمز عبور حساب‌های کاربری سرویس

همانطور که از نام این حساب‌های کاربری پیداست، برای راه‌اندازی سرویس‌های مورد نیاز در ساختار مانند SQL و غیره از این حساب‌های کاربری استفاده می‌شود. اما نکته‌ای که از لحاظ امنیتی در این حساب‌های کاربری حائز اهمیت است Expire شدن رمزعبور این حساب‌های کاربری است. اکثر مدیران عموماً برای حساب‌های کاربری مرتبط به سرویس امکان Expire شدن آن‌ها را غیرفعال می‌کنند تا درگیر تعویض متناوب رمز عبور نشوند. اگر چه رویارویی با این مشکل دشواری‌های خاص خود را دارد، اما راهکارهایی به منظور ایمن‌سازی این حساب‌های کاربری پیشنهاد می‌شود. برای این منظور می‌توان تمام حساب‌های کاربری مرتبط به سرویس‌ها را در یک گروه واحد و OU مجتمع کرده و سیاست Allow Logon Locally را برای رایانه Server های برنامه‌های کاربردی غیرفعال نموده و Log on as service را فعال نمایید.

اخبار داخلی

وبینـــار تاکتیـــک‌های تیـــم قـــرمز در امنـــیت ســـایبری

تیم قرمز (Red Teams): تیم قرمز، تیم آموزش‌دیده‌ای 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 به صورت 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. در این وبینار تاکتیک‌هایی که تیم قرمز به کار می‌برند و تفاوت رنگ در تیم‌های امنیت سایبری برای شرکت‌کنندگان اعم از دانشجویان، پرسنل IT سازمان‌ها و شرکت‌ها و علاقمندان این حوزه ارائه گردید.

ثبت‌نـــام دوره‌هـــای آنـــلاین مـــرکز تخصصـــی آپـــا

ثبت‌نام دوره‌های آنلاین، امنیت شبکه CCNA Security، هکر قانونمند CEHv11 و دوره حرفه‌ای شبکه سیسکو CCNP Enterprise ENCOR 350-401 مرکز آپا اغاز گردید. پس از پایان دوره به افرادی که با موفقیت دوره را به پایان برسانند مدرک معتبر مورد تأیید سازمان فناوری اطلاعات (نما) و افتای ریاست جمهوری اعطاء می‌گردد. جزییات هر یک از دوره‌ها به صورت کامل در لینک زیر ذکر شده است:

https://evand.com/events/raziapa-99

۱- دوره هکر قانونمند CEHv10

مدرک CEH یکی از معتبرترین مدارک شرکت EC-Council می‌باشد. دوره CEH بر روی تکنیک‌ها و تکنولوژی‌های هک از دیدگاه حمله تکیه می‌کند. در دور CEH، دانشجویان با چک‌لیست‌های امنیتی آشنا شده و توانایی بررسی سیستم‌های امنیتی موجود را کسب می‌نمایند و قادر به شناسایی آسیب‌پذیری‌های سیستم و تعیین وضعیت امنیتی یک سازمان با استفاده از تست‌های نفوذ هستند. همچنین با استفاده از حمله به سیستم‌ها، روش‌های دفاعی نیز مورد بررسی قرار خواهند گرفت.

۲- دوره امنیت شبکه سیسکو CCNA Security

در این دوره افراد با تجهیزات امنیتی سیسکو آشنا می‌شوند .به طوری که بتوانند بر روی یک شبکه متوسط در لایه های ۲ و ۳ امنیت ایجاد کنند. در واقع این دوره گام اول ورود به دنیای امنیت سیسکو می‌باشد. مدرک CCNA Security تأیید می‌کند شما دانش و مهارت لازم برای تامین امنیت شبکه‌های سیسکو را دارید. همچنین بیانگر این است که شما توانایی شناسایی انواع حملات و تهدیدهای شبکه را دارید و می‌توانید از شبکه خود در مقابل آن‌ها محافظت نمایید .استاندارد آموزشی این دوره شامل تکنولوژی‌های امنیتی، نصب و عیب‌یابی و مانیتورینگ تجهیزات شبکه جهت اعمال availability، Confidentiality، Integrity داده‌ها می‌باشد. لازم به ذکر است این دوره به صورت آنلاین برگزار می‌گردد.

۳- دوره حرفه ای شبکه سیسکو CCNP Enterprise ENCOR 350-401

دوره CCNP تایید توانایی شما برای طراحی، پیاده‌سازی، بررسی و عیب‌یابی شبکه‌های محلی و گسترده سازمانی است. گواهینامه CCNP برای افرادی که حداقل یکسال تجربه کار در زمینه شبکه دارند و آماده پیشرفت مهارت‌هایشان هستند مناسب است .در این دوره برنامه‌ریزی، ترکیب‌بندی و بررسی پیاده‌سازی راه حل‌های سوییچنگ و روتینگ سازمان با استفاده از معماری Campus را فرا خواهید گرفت.

اخبار کوتاه

هشدار وسترن دیجیتال: بلافاصله درایوهای My Book Live خود را قطع کنید

وسترن دیجیتال از مشتریان خود می‌خواهد هارددیسک My Book Live را از اینترنت جدا کنند تا از پاک شدن داده‌ها توسط بدافزار جلوگیری کنند.

به نظر می‌رسد هکرها از یک آسیب‌پذیری که برای اولین بار در سال ۲۰۱۹ منتشر شده بود، استفاده می‌کنند. Western Digital در سال ۲۰۱۵ پشتیبانی از درایوهای My Live را متوقف کرد و از آن زمان سیستم‌عامل خود را به‌روز نکرده است.

این شرکت نوشت: وسترن دیجیتال تشخیص داده است که برخی از دستگاه‌های My Book Live و My Book Live Duo از طریق سوءاستفاده از آسیب‌پذیری اجرای دستور از راه دور به خطر می‌افتند. در برخی موارد، این سازش منجر به بازنشانی کارخانه شده است که به نظر می‌رسد تمام داده‌های دستگاه را پاک می‌کند." این مسئله در حالی آشکار شد که کاربران My Book Live و My Book Live Duo از انجمن شرکت به خاطر درایوهایشان شکایت کرده‌اند.

یکی از کاربران نوشت: "من بدون این داده‌هایم سال‌ها گیج و عصبانی خواهم بود."

دیگری نوشت: "تقریباً تمام روز در این باره حرص خوردم." "من از هفت ماه پیش کار جدیدی را شروع کردم و تمام داده‌های کارم در این مدت در اینجا بود."

وسترن دیجیتال در پستی درباره این موضوع گفت که آن‌ها در حال بررسی این مشکل هستند. "ما درک می‌کنیم که داده‌های مشتریان ما بسیار مهم است. ما به طور فعال در حال بررسی این موضوع هستیم و وقتی اطلاعات بیشتری بدست بیاوریم؛ یک مشاوره به روز ارائه خواهیم داد."

ثبت‌نام دوره‌های آنلاین مرکز آپا دانشگاه رازی

دوره هکر قانونمند
CEH V11

مهندس شهاب ارکان

۴۵ ساعت

چهارشنبه‌ها | ۱۷:۳۰ الی ۲۰

دوره حرفه‌ای شبکه سیسکو
CCNP Enterprise Core
ENCOR 350-401

مهندس سعید زنگنه

۶۰ ساعت

شنبه‌ها | ۱۷ الی ۲۰

دوره امنیت شبکه سیسکو
CCNA Security

مهندس شهاب ارکان

۴۰ ساعت

یکشنبه‌ها | ۱۷ الی ۲۰

برای دانشجویان
۲۰% تخفیف

تخفیف پلکانی برای دانش‌پذیران دوره‌های آپا

دوره‌ها منطبق با سرفصل‌های استاندارد تدریس می‌گردند.

همراه با ارائه مدارک معتبر

با اساتیدی مجرب

ظرفیت محدود

لینک ثبت‌نام:

evand.com/events/raziapa-99

<راه‌های ارتباطی>

cert.razi.ac.ir

۰۸۳۳۴۳۴۳۲۵۱

APARazi

APA_Razi

Firefox