بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره سی‌و یکم

مردادماه ۱۴۰۰

وردپرس

هدف مورد علاقه‌ی هکرها!

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:

مرکز تخصصـــی آپـا دانشگـاه رازی

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

همکاران این شماره:

سهیلا مرادی

صبا آزرمی

سیده آرزو حسنی

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

سرورهای Exchange تحت حملات ناشی از آسیب‌پذیری‌های ProxyShell

یک محقق در Black Hat نشان داد که شکل جدیدی از حمله بر روی سرورهای Exchange وجود دارد و مهاجمان اکنون در حال سوءاستفاده از سرورهای آسیب‌پذیر در برابر باگ‌های RCE هستند.

هانی‌پات‌های Exchange server محققانِ مایکروسافت به صورت فعال توسط ProxyShell مورد حمله قرار می‌گیرند. ProxyShell نام حمله‌ای است که هفته گذشته در Black Hat فاش شد و سه آسیب‌پذیری را شامل می‌شود. این آسیب‌پذیری‌ها مهاجمان احراز هویت‌نشده را قادر می‌سازند از راه دور کد دلخواه خود را اجرا نمایند (RCE) و بتوانند پسوردها را به صورت متن ساده ببینند.

Orange Tsai محقق امنیتی Devcore، در ارائه‌ی هفته پیش خود در Black Hat گفت بررسی‌ها نشان می‌دهد بیش از ۴۰۰،۰۰۰ Exchange server روی اینترنت وجود دارند که از طریق پورت ۴۴۳ در معرض حمله قرار گرفته‌اند. روز دوشنبه، Jan Kopriva از SANS Internet Storm Center گزارش داد که وی بیش از ۳۰،۰۰۰ سرور Exchange آسیب‌پذیر را از طریق اسکن Shodan یافته است و هر مهاجمی که بخواهد از این طریق اقدام کند با اطلاعات زیادی که در اختیار دارد می‌تواند در یک اقدام سریع از این آسیب‌پذیری سوءاستفاده نماید. طبق محاسبات توثیت شده توسط یک محقق امنیتی به نام Kevin Beaumont و طبق جستجوهای Shodan، این بدان معناست که بین ProxyLogon و ProxyShell تنها ۵۰ درصد سرورهای Exchange در حال حاضر در معرض خطر بهره‌برداری قرار دارند.

البته، مایکروسافت برای تمام آسیب‌پذیری‌های موردنظر وصله‌های امنیتی منتشر کرده است و به گفته‌ی Kopriva، به احتمال زیاد اکثر سازمان‌هایی که تا حدودی امنیت را جدی می‌گیرند تا کنون وصله‌ها را اعمال کرده‌اند.

این آسیب‌پذیری‌ها Exchange Server نسخه‌های ۲۰۱۳، ۲۰۱۶ و ۲۰۱۹ را تحت تأثیر قرار می‌دهد.

روز پنجشنبه، Beaumont و محقق گروه NCC به نام Rich Warren، فاش کردند که مهاجمان با استفاده از آسیب‌پذیری ProxyShell هانی‌پات‌های Exchange server

آن‌ها را مورد حمله قرار داده و توانسته‌اند از آن‌ها بهره‌برداری نمایند. Warren با عکسی از کد c# aspx webshell که در دایرکتوری /aspnet_client/ وجود داشت توئیت کرد:"آغاز تلاش‌های گسترده علیه زیرساخت‌های هانی‌پات ما برای آسیب‌پذیری‌های Exchange ProxyShell".

مانور خطرناک بر روی شکل جدید حمله

Tsai در پستی در روز یکشنبه بازگو کرد که کد اثبات مفهومی ProxyLogon که Devco در اواخر فوریه به MSRC گزارش کرد، به ما می‌گوید که این امر محققان را نیز مانند سایرین پس از حذف احتمال نشت اطلاعات از طرف ما و از طریق تحقیقات کنجکاو کرد. وی ادامه داد: "با ظاهر شدن جداول زمانی واضح‌تر و بحث بیشتر، به نظر می‌رسد این اولین بار نیست که چنین چیزی برای مایکروسافت اتفاق می‌افتد."سرور ایمیل هم یک دارایی بسیار ارزشمند است و هم ظاهراً برای مهاجمان یک هدف قوی و مهم است، چرا که اسرار محرمانه و داده‌های شرکت‌ها را حفظ می کند.

Tsai تشریح کرد: "به عبارت دیگر، کنترل سرور ایمیل به معنای کنترل حیات یک شرکت است." Exchange Server به عنوان یک راهکار رایج و متداول برای مدیریت ایمیل ها، مدت‌هاست که هدف اصلی هکرها قرار گرفته است. بر اساس تحقیقات صورت گرفته، بیش از چهارصد هزار Exchange Server در بستر اینترنت وجود دارند. هر سرور نماینده یک شرکت است و حتماً می‌توانید تصور کنید اینکه یک آسیب‌پذیری خطرناک در Exchange Server کشف شده است چقدر می‌تواند وحشتناک باشد."

Tsai در ارائه خود در Black Hat تشریح کرد که تیم وی این شکل جدید حمله را براساس یک تغییر چشمگیر که در Exchange Server 2013 صورت گرفته بود کشف کرده است. جایی که کنترل‌کننده‌ی اصلی پروتکل یعنی Client Access Service (CAS) در frontend و backend جدا می‌شود_ یک تغییر که شامل طراحی بسیار زیادی بود و ۸ آسیب‌پذیری را به همراه داشت که شامل نقص‌های سمت سرور، سمت کلاینت و نقص‌های رمزنگاری بود.

وی این نقص‌ها را به سه روش حمله نسبت داد:

ProxyLogon که به بدنامی مشهور است و موجب انتشار وصله‌ی چندماه پیش شد و هم‌اکنون نیز در معرض حملات فعال قرار دارد و روش دیگر حمله که ProxyOracle نامیده می‌شود. این شیوه‌های حمله هر مهاجم احرازهویت‌نشده‌ای را قادر می‌سازند که پسوردهای متن‌ساده را کشف کرده و حتی کدهای دلخواه خود را در Microsoft Exchange Server بر روی پروت ۴۴۳ اجرا نماید.

سه آسیب‌پذیری که Tsai آن‌ها را به ProxyLogon نسبت داد و همه‌ی آن‌ها در حال حاضر وصله شده‌اند عبارتند از:

CVE-2021-34473: Pre-auth path confusion که دور زدن ACL را منجر می‌شود.

CVE-2021-34523: ارتقاء سطح دسترسی در یک اِندِ Exchange PowerShell.

Post-auth arbitrary file-write : که اجرای حمله از راه دور را منجر می‌شود.

نقص ProxyShell موجب شد تیم Devcore پس از تسخیر Exchange server با استفاده از این باگ، در مسابقات Pwn2Own ۲۰۲۱ که در ماه آوریل برگزار شد ۲۰۰,۰۰۰ دلار جایزه بگیرند.

Tsai در صحبت با Black Hat گفت که وی آسیب‌پذیری‌های Exchange را زمانی که Microsoft Exchange CAS را هدف قرار داده کشف کرده است و طبق این توضیحات، CAS یک مؤلفه‌ی اساسی در Exchange محسوب می‌شود. Tsai در این صحبت به اسناد مایکروسافت اشاره کرد که در آن‌ها آمده است:

"سرورهای Mailbox حاوی سرویس‌های Client Access هستند که ارتباطات مشتری را برای تمام پروتکل‌ها می‌پذیرند. سرویس‌های frontend مسئول مسیریابی یا پراکسی ارتباطات به سرویس‌های backend مربوطه در سرور Mailbox هستند."با توجه به این موضوع می‌توانید به اهمیت CAS پی ببرید و می‌توانید تصور کنید که پیدا شدن آسیب‌پذیری در چنین زیرساخت‌هایی تا چه اندازه می‌تواند حائز اهمیت باشد. Tsai می‌گوید با این تفاسیر CAS جایی بود که ما روی آن تمرکز کردیم و این شکل حمله ظاهر شد. بنابراین CAS یک مؤلفه‌ی اساسی در پذیرش ارتباطات سمت کلاینت صرف‌نظر از پروتکل‌های HTTP، POP3، IMAP یا SMTP است و ارتباطات را به سرویس backend مربوطه پراکسی می‌کند.

ProxyShell تنها نوک کوه یخ!

از میان تمام نقص‌های یافت‌شده در این شکل جدید حمله، Tsai آسیب‌پذیری CVE-2020-0688 (یک آسیب‌پذیری اجرای کد از راه دور که یک کلید رمزنگاری hard-code را در Exchange درگیر می‌کرد) "شگفت‌انگیزترین" نامید.

وی نوشت: "با این کلید hard-code شده مهاجمی با سطح دسترسی پایین می‌تواند تمام Exchange Server را تحت کنترل بگیرد." و همانطور که می‌بینید حتی در سال ۲۰۲۰ هم یک کلید رمزنگاری hard-code شده و احمقانه همچنان در نرم‌افزارهای مهمی مانند Exchange یافت می‌شوند. این نشان می‌دهد که Exchange فاقد بررسی‌های امنیتی است و به من انگیزه داد تا بیشتر در مورد امنیت Exchange کند و کاو کنم."

Tsai گفت که "جالب‌ترین" نقص، CVE-2018-8581 است که توسط شخصی که با ZDI همکاری می‌کرد کشف شد. وی اظهار داشت اگرچه این آسیب‌پذیری یک نقص جعل درخواست ساده در سمت سرور (SSRF) است، اما می‌تواند با NTLM Relay ترکیب شده و مهاجم را قادر سازد که یک SSRF خسته‌کننده را به چیزی واقعاً فانتزی تبدیل کند." به عنوان مثال، مهاجم می‌تواند به طور مستقیم کنترل تمام Domain Controller را از طریق یک حساب کاربری با سطح دسترسی پایین در دست بگیرد.

منبع خبر :

Scan Link

هشـــدار مایکروســـافت در خصوص spear-phishing

شرکت مایکروسافت فاش کرد که از ماه ژوئیه ۲۰۲۰ یک کمپین فیشینگ هدفدار[۱]، مشتریان Office 365 را مورد حمـله قرار می‌دهند. در این حمـلات، مهاجمان از پیوست‌های[۲] XLS.HTML استفاده کرده‌اند، به این صورت که این پیوست‌ها به چندین بخش مختلف از جمله فایل‌های جاوا اسکریپت جهت سرقت گذرواژه‌ها تقسیم می‌شوند که سپس با استفاده از مکانیزم‌های مختلف رمزگذاری می‌شوند. مایکروسافت گزارش داد که مهاجمان به طور متوسط هر ۳۷ روز یک بار مکانیزم رمزگذاری را تغییر می‌دهند تا از این طریق، حملات آن‌ها قابل ردیابی و قابل تشخیص نباشد. همچنین مهاجمان جهت مخفی کردن حملات خود، از تکنیک‌های رمزگذاری مختلفی از جمله روش‌های غیرمعمول و قدیمی رمزگذاری مانند کد Morse، استفاده می‌کنند.

بر اساس گزارش منتشر شده از تیم Microsoft 365 Defender Threat Intelligence، برخی از بخش‌های کد، در خود پیوست وجود ندارند و در عوض در دایرکتوری‌های باز، تحت عنوان اسکریپت‌های رمزشده قرار دارند. مهاجمان پیوست‌های HTML را در بخش‌های جداگانه‌ای که به ظاهر مخرب نیستند قرار می‌دهند تا از این طریق تدابیر امنیتی را دور بزنند؛ این بخش‌ها شامل موارد زیر می‌باشند:

بخش ۱: آدرس ایمیل هدف

بخش ۲: لوگوی سازمان هدف، از:

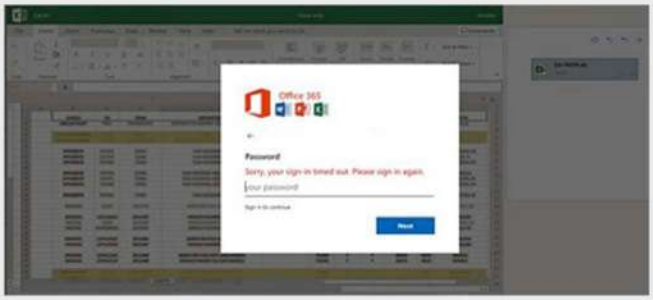
logo[.]clearbit[.]com, i[.]gyazo[.]com, or api[.]statvoo[.]com

اگر لوگو در دسترس نباشد، به جای آن، لوگوی Microsoft Office 365 بارگذاری می‌شود.

بخش ۳: اسکریپتی که تصویر یک سند تار و مبهم را بارگذاری می‌کند و نشان می‌دهد که ورود به سیستم به پایان رسیده است.

بخش ۴: اسکریپتی که کاربر را ترغیب به وارد کردن گذرواژه خود می‌کند تا گذرواژه وارد شده از راه دور به یک کیت فیشینگ ارسال شده و یک صفحه جعلی با پیام خطا به کاربر نمایش داده شود.

مهاجم با فریب کاربر نسبت به راه‌اندازی فایل پیوست، همانند تصویر زیر یک صفحه‌ی ورود جعلی بر روی برنامه اکسل که زمینه‌ی آن تار است، به وی نمایش می‌دهد و از کاربر قربانی می‌خواهد که نام کاربری و رمز عبور خود را برای مشاهده سند آفیس وارد کند، در این صورت اگر کاربر رمز عبور خود را وارد کند برای وی اسکریپت هشداری بر روی صفحه نمایش داده می‌شود و به قربانی اطلاع می‌دهد که رمز عبور وارد شده اشتباه است که در واقع از این طریق رمز عبور برای مهاجم ارسال خواهد شد.



کارشناسان امنیتی معتقدند که هدف مهاجمان از این حملات آن است که اطلاعاتی نظیر نام کاربری، رمزعبور، آدرس IP و موقعیت مکانی کاربر را که می‌تواند در حملات بعدی مورد استفاده قرار گیرد، به دست آورند. گفتنی است که مایکروسافت، IoCs[۳] مرتبط با این حملات را منتشر کرده است.

منبع خبر :

Scan Link

ســـایت‌های وردپرســی در معـــرض حمـــلات فیشیـــنگ

یک کمپین فیشینگ هدفدار به نام Aggah مرتبط با پاکستان از سایت‌های وردپرسی که در معرض خطر هستند جهت تزریق بدافزار Warzone RAT به شرکت‌های تولید کننده در تایوان و کره جنوبی سوءاستفاده می‌کند. بدافزار Warzone RAT می‌تواند در نهایت منجر به ارتقاء سطح دسترسی keylogging، امکان دسترسی به shell از راه دور، دانلود و اجرای فایل‌ها، مدیریت فایل‌ها و استقرار در شبکه شود. این افزایش سطح دسترسی از طریق بدافزار Warzone با استفاده از فایل sdclt.exe که یک ابزار پشتیبانی در ویندوز ۱۰ است، انجام می‌شود.

این کمپین که در اوایل ماه ژوئیه ۲۰۲۱ فعالیت خود را آغاز کرد، از آدرس‌های ایمیل جعلی جهت انجام حملات خود سوءاستفاده می‌کند. مهاجمان اغلب تولیدکنندگان جهانی و سایر تأمین کنندگان را نه تنها برای آسیب‌رساندن به آن‌ها، بلکه به عنوان راهی جهت نفوذ به برخی از مشتریان مورد نظر خود هدف قرار می‌دهند.

به گفته محققان، کمپین فیشینگ هدفدار، کار خود را با ارسال یک ایمیل سفارشی با نام "FoodHub.co.uk" مبنی بر یک سرویس تحویل آنلاین غذا که در انگلستان مستقر است، شـروع می‌کند. محـتوای ایمیـل شـامل یک فایل پاورپوینت با نام Purchase order 4500061977,pdf.ppam است که شامل ماکروهای مبهمی است که از فایل mshta.exe جهت اجرای جاوا اسکریپت یک سایت خطرناک استفاده

---

[۱] spear-phishing
[۲] Attachments
[۳] Indicators of Compromise

می‌کند. در حملات صورت گرفته، جاوا اسکریپت از PowerShell جهت بارگذاری پی‌لودهای hex-encoded استفاده می‌کند.

طی بررسی‌های صورت گرفته توسط محققان، مهاجمان از وب‌سایت‌های قانونی جهت اجرای اسکریپت‌های مخرب استفاده می‌کنند که به نظر می‌رسد بیشتر این وب‌سایت‌ها وردپرس هستند، این امر نشان‌دهنده آن است که کمپین مذکور، ممکن است از آسیب‌پذیری وردپرس سوء استفاده کرده باشد.

منبع خبر :

Scan Link

باج افزارها می‌توانند به‌سرعت نفوذ کرده و به سازمان‌ها آسیب جدی برسانند

Cloudian گزارش Ransomware Victims Report 2021 خود را بر اساس یک نظرسنجی مستقل از ۲۰۰ تصمیم‌گیرنده فناوری اطلاعات که سازمان‌هایشان از سال ۲۰۱۹ تا ۲۰۲۱ حمله‌های باج‌افزاری را تجربه کرده‌اند، ارائه داده است.

این بررسی نشان داد که ابزارهای دفاعی که در برابر حملات باج افزار مورداستفاده قرار می‌گیرند در حال شکست می‌باشند، به‌طوری‌که ٪۵۴ از کل قربانیان آموزش‌های ضد فیشینگ را دیده و ٪۴۹ آن‌ها ابزارهای دفاعی در زمان حمله را دارا بودند. با استناد به این یافته و سایر یافته‌های این بررسی نشان‌دهنده تأثیر گسترده حملات و متوسط هزینه‌های مالی بالغ بر ۴۰۰۰۰۰ دلار است. این گزارش از سازمان‌ها می‌خواهد تا توجه بیشتری را بر روی فراهم کردن دستگاه‌هایی بگذارند که بازیابی سریع اطلاعات در صورت حمله را بدون پرداخت ضرر فراهم می‌کنند.

باوجود اقدامات دفاعی، باج افزار وارد می‌شود

بسیاری از سازمان‌ها بخش عمده‌ای از بودجه امنیت سایبری خود را صرف اقدامات دفاعی مانند نرم‌افزار ضد بدافزار و آموزش ضد فیشینگ برای کارمندان می‌کنند. باوجود این تلاش‌ها، حملات باج افزار به‌طور فزاینده‌ای پیچیده‌تر شده و مجرمان سایبری را قادر می‌سازد به سیستم دفاعی نفوذ کنند. این بررسی نشان داد که:

- فیشینگ همچنان یکی از آسان‌ترین مسیرهای باج افزار است که ٪۲۴ حملات باج‌افزار از این طریق شروع می‌شود.
- با جود این واقعیت که ٪۵۴ از کل پاسخ‌دهندگان و ٪۶۵ از کسانی که آن را به‌عنوان نقطه ورود گزارش داده بودند، آموزش ضدفیشینگ را برای کارمندان انجام داده بودند، بازهم باج‌افزار موفق به ورود از طریق فیشینگ شد.
- ٪۴۹ از پاسخ‌دهندگان قبل از حمله موفقیت‌آمیز ابزار دفاعی داشتند.
- فضای ابر عمومی رایج‌ترین نقطه ورود باج‌افزار بود، ٪۳۱ پاسخ‌دهندگان از این طریق موردحمله قرار گرفتند.

مهاجمان سریع حرکت می‌کنند

هنگامی‌که مجرمان اینترنتی قادر به درج باج‌افزار شدند، می‌توانند به‌سرعت بر محیط تسلط یابند و به‌طور قابل‌توجهی بر تمام جنبه‌های سازمان تأثیر بگذارند:

- ٪۵۶ از پاسخ‌دهندگان به نظرسنجی گزارش دادند که مهاجمان فقط در مدت ۱۲ ساعت قادر به کنترل اطلاعات و درخواست وجه بودند و ٪۳۰ دیگر گفتند که این اتفاق در عرض ۲۴ ساعت رخ‌داده است.
- بیش از نیمی از شرکت‌کنندگان در این نظرسنجی گفتند که این حملات به‌طور قابل توجهی بر امور مالی، عملیاتی، کارمندان، مشتریان و اعتبار آن‌ها تأثیر می‌گذارد.

هزینه‌های مالی واردشده بر سازمان فراتر از مبلغ درخواست شده توسط باج‌افزارها می‌باشد. پرداخت هزینه به مهاجمان به‌صورت قابل‌توجه در حال افزایش است، اما تنها چنین مبالغی هزینه‌های این حملات نیستند. برای ٪۵۵ پاسخ‌دهندگانی که پرداخت هزینه مالی را انتخاب کرده‌اند:

- متوسط پرداخت مبلغ به مهاجمان ۲۲۳۰۰۰ دلار بود که ٪۱۴ آن‌ها ۵۰۰۰۰۰ دلار یا بیشتر پرداخت کرده‌اند.
- آن‌ها به‌طور متوسط ۱۸۳۰۰۰ دلارید بیشتر برای سایر هزینه‌های ناشی از حمله هزینه کرده‌اند.
- بیمه تنها حدود ٪۶۰ از پرداخت باج افزار و سایر هزینه‌ها را پوشش می‌دهد که احتمالاً منعکس‌کننده کسر هزینه‌ها و محدودیت‌های پوشش است.
- باوجود پرداخت مبلغ به مهاجمان، فقط ٪۵۷ از پاسخ‌دهندگان تمام داده‌های خود را پس گرفتند.

Jon Toor، مدیر CMO،Cloudian گفت: "تهدید باج‌افزار همچنان سازمان‌های سراسر جهان را آزار خواهد داد." "حملات سایبری می‌توانند حتی در قوی‌ترین موارد دفاعی نیز نفوذ کنند، بنابراین بسیار مهم است که سازمان‌ها توانایی بهبودی سریع پاسخ به حمله را در اولویت خود داشته باشند. بهترین راه این است که یک نسخه پشتیبان غیرقابل تغییر از داده‌های خود داشته باشید که از رمزگذاری یا حذف داده‌ها برای مدت‌زمان مشخصی توسط هکرها جلوگیری می‌کند. درنتیجه، سازمان‌ها می‌توانند در صورت حمله بدون نیاز به پرداخت هزینه، کپی رمزنگاری نشده از داده‌های خود را بازیابی کنند.

منبع خبر :

Scan Link

آسیب پذیری

آسیب‌پذیری‌های بحرانی در VPN Routerهای سیسکو

محققان امنیتی هشدار دادند که حداقل ۸۸۰۰ دستگاه آسیب‌پذیر وجود دارد که در معرض خطر تسخیر قرار دارند. یک آسیب‌پذیری امنیتی با شدت بحرانی در زیرمجموعه ای از روترهای Small-business VPN router سیسکو به مهاجم احراز هویت نشده از راه دور اجاز می‌دهد کنترل دستگاه را در دست بگیرد.

سیسکو این آسیب‌پذیری را که شناسه CVE-2021-1609 به آن اختصاص داده شده، به عنوان بخشی از وصله‌های امنیتی که این هفته منتشر شده است برطرف نمود. در مجموع، آسیب‌پذیری‌های رفع شده و نسخه‌های تحت تأثیر به شرح زیر می‌باشند:

- آسیب‌پذیری‌های مدیریت وب در سری‌های RV345، RV340W، RV340 و RV345P از مدلDual WAN Gigabit VPN Routers روترهای سیسکو
- آسیب‌پذیری اجرای کد از راه دور در VPN Routerهای سری RV160 و RV260
- آسیب‌پذیری تزریق DLL ویندوز برای نرم‌افزار Cisco Packet Tracer
- آسیب‌پذیری ارتقاء سطح دسترسی بر روی CLI Secure Shell Server در Cisco Network Services Orchestrator
- آسیب‌پذیری ارتقاء سطح دسترسی بر روی CLI Secure Shell Server در ابزار ConfD سیسکو

آسیب‌پذیری اجرای کد از راه دور در Gigabit VPN Routers

این نقص بحرانی VPN routerهای مدل Dual WAN Gigabit را تحت تأثیر قرار می‌دهد. این آسیب‌پذیری در رابط مدیریت تحت‌وب این دستگاه‌ها وجود دارد و با شدت بحرانی (۹.۸ از ۱۰) در سیستم CVSS3 امتیازدهی می‌شود. دلیل وجود این نقص اعتبارسنجی نامناسبِ درخواست‌های HTTP می‌باشد.

براساس تجزیه و تحلیل Tenable، یک مهاجم از راه دور می‌تواند بدون احراز هویت با ارسال درخواست‌های HTTP ساختگی به دستگاه آسیب‌پذیر، از این آسیب‌پذیری بهره برداری نماید. این امر منجر به اجرای کد دلخواه و همچنین ریستارت شدن دستگاه می‌شود که نتیجه‌ی آن ممانعت از سرویس‌دهی یا همان حمله‌ی DoS است.

به گفته‌ی سیسکو، قابلیت مدیریت از راه دور در این دستگاه‌ها به طور پیش‌فرض غیرفعال است که چنین حملاتی را خنثی می‌کند. با این وجود، محققان Tenable، ۸۸۰۰ دستگاه را یافتند که به صورت عمومی در دسترس بوده و در مقابل این حمله آسیب‌پذیر می‌باشند.

آسیب‌پذیری وصله‌نشده در Fortinet امکان تسخیر فایروال را فراهم می‌کند!

این آسیب‌پذیری یک نقص OS command-injection در فایروال وب‌اپلیکیشن (WAF) موسوم به FortiWeb است که امکان ارتقاء سطح دسترسی و در نهایت تسخیر دستگاه را برای مهاجم فراهم می‌کند.

FortiWeb یک پلتفرم دفاعی امنیت سایبری است که هدف آن محافظت از برنامه‌های کاربردی تحت‌وب در برابر حملاتی است که آسیب‌پذیری‌های شناخته شده و ناشناخته را هدف قرار می‌دهند. به گفته‌ی Fortinet، این فایروال با قابلیت‌های جدید یا به‌روزشده و همچنین APIهای وب جدید هماهنگ است.

به گفته‌ی William Vu محقق Rapid7، که این نقص را کشف کرده است، این آسیب‌پذیری که در حال حاضر CVE به آن اختصاص داده نشده است، در رابط مدیریت FortiWeb (برای نسخه‌های ۶.۳.۱۱ و قبل از آن) وجود دارد و با درجه شدت ۸.۷ از ۱۰ از آسیب‌پذیری‌های دارای شدت بالا محسوب می‌شود. این نقص به مهاجم احراز هویت‌شده از راه دور اجازه می‌دهد از طریق صفحه پیکربندی SAML Server دستورات دلخواه خود را در سیستم اجرا نماید.

توجه داشته باشید اگرچه لازمه‌ی بهره‌برداری از این نقص احراز هویت است و تنها هکرِ احراز هویت‌شده می‌تواند آن را مورد بهره‌برداری قرار دهد، اما این نقص می‌تواند با یک آسیب‌پذیری دور زدن فرایند احراز هویت مانند CVE-2020-29015 ترکیب شده و کار را برای مهاجم آسان کند.

مهاجمان به محض احرازهویت شدن در رابط مدیریت دستگاه FortiWeb قادر خواهند بود دستورات دلخواه خود را با استفاده از backticks در فیلد "Name" در صفحه پیکربندی SAML Server اجرا نمایند. این دستورات به عنوان کاربر root در سیستم‌عامل اجرا خواهند شد.

مهاجم می‌تواند از این آسیب‌پذیری برای کنترل کامل دستگاه آسیب‌پذیر با بالاترین سطح دسترسی ممکن استفاده کند. مهاجم ممکن است یک shell دائمی، یک نرم‌افزار استخراج رمزارز یا سایر نرم‌افزارهای مخرب را در دستگاه آسیب‌پذیر نصب کند.

اگر رابط مدیریت این دستگاه از طریق اینترنت در دسترس باشد آسیب می‌تواند بدتر و خطرناک‌تر باشد. Rapid7 خاطرنشان کرد که در این صورت مهاجمان به شبکه گسترده‌تری دسترسی دارند. با این حال، محققان Rapid7 تاکنون ۳۰۰ دستگاه را شناسایی کرده‌اند که رابط مدیریت آن‌ها از طریق اینترنت در دسترس است.

در این تجزیه و تحلیل‌ها، Vu یک کد اثبات مفهومی (PoC) ارائه نمود که از درخواست و پاسخ HTTP POST استفاده می‌کند. با توجه افشای این خبر، Fortinet که قصد داشت این نقص را در پایان ماه آگوست در نسخه ۶.۴.۱ برطرف کند، این اقدام را در اولویت قرار داده و احتمالاً تا پایان این هفته نسخه‌ی به‌روزشده‌ی آن در دسترس خواهد بود.

محققان Rapid7 می‌گویند به نظر می‌رسد این آسیب‌پذیری مربوط به CVE-2021-22123 باشد که در ماه ژوئن وصله شد.

توصیه امنیتی:

Rapid7 به کاربران توصیه می‌کند تا زمان انتشار نسخه‌ی به‌روزشده، کاربران رابط مدیریت دستگاه FortiWeb را برای شبکه‌های غیرقابل اعتماد که اینترنت را هم می‌تواند شامل شود غیرفعال کنند. البته به طور کلی، رابط‌های مدیریت دستگاه‌هایی مانند FortiWeb به هر حال نباید مستقیماً از طریق اینترنت در دسترس باشند- رابط مدیریت این دستگاه‌ها فقط باید از طریق شبکه‌های داخلی قابل اعتماد یا از طریق اتصال VPN امن قابل دسترسی باشند.

منبع خبر :

Scan Link

آسیب‌پذیری XSS در افزونه SEOPress وردپرس امکان تسخیر سایت را فراهم می‌کند

این آسیب‌پذیری می‌تواند موجب اقدامات مخربی از جمله تسخیر سایت شود. این افزونه ی آسیب‌پذیر بر روی ۱۰۰،۰۰۰ وب‌سایت نصب شده است.

به گفته‌ی محققان، آسیب‌پذیری stored cross-site scripting (XSS) در افزونه‌ی SEOPress، به مهاجمان اجازه می‌دهد اسکریپت‌های وب دلخواه خود را به وب‌سایت‌ها تزریق کنند.

SEOPress یک ابزار بهینه‌سازی موتورهای جستجو (SEO) است که امکان مدیریت متادیتای SEO، کارت‌های social-media، تنظیمات Google Ad و سایر موارد را به مدیران سایت می‌دهد. محققان Wordfence در یک پست وبلاگی در روز دوشنبه گفتند: "یکی از ویژگی‌های این افزونه امکان افزودن عنوان SEO و توضیحات به پست‌ها است و این می‌تواند هنگام ذخیره‌ی ویرایش‌ها در یک پست یا از طریق REST-APIهای اخیراً معرفی‌شده انجام شود."متأسفانه این REST-API endpoint به صورت ناامن

آسیب‌پذیری وصله‌نشده در Fortinet امکان تسخیر فایروال را فراهم می‌کند!

این آسیب‌پذیری یک نقص OS command-injection در فایروال وب‌اپلیکیشن (WAF) موسوم به FortiWeb است که امکان ارتقاء سطح دسترسی و در نهایت تسخیر دستگاه را برای مهاجم فراهم می‌کند.

FortiWeb یک پلتفرم دفاعی امنیت سایبری است که هدف آن محافظت از برنامه‌های کاربردی تحت‌وب در برابر حملاتی است که آسیب‌پذیری‌های شناخته شده و ناشناخته را هدف قرار می‌دهند. به گفته‌ی Fortinet، این فایروال با قابلیت‌های جدید یا به‌روزشده و همچنین APIهای وب جدید هماهنگ است.

به گفته‌ی William Vu محقق Rapid7، که این نقص را کشف کرده است، این آسیب‌پذیری که در حال حاضر CVE به آن اختصاص داده نشده است، در رابط مدیریت FortiWeb (برای نسخه‌های ۶.۳.۱۱ و قبل از آن) وجود دارد و با درجه شدت ۸.۷ از ۱۰ از آسیب‌پذیری‌های دارای شدت بالا محسوب می‌شود. این نقص به مهاجم احراز هویت‌شده از راه دور اجازه می‌دهد از طریق صفحه پیکربندی SAML Server دستورات دلخواه خود را در سیستم اجرا نماید.

توجه داشته باشید اگرچه لازمه‌ی بهره‌برداری از این نقص احراز هویت است و تنها هکرِ احراز هویت‌شده می‌تواند آن را مورد بهره‌برداری قرار دهد، اما این نقص می‌تواند با یک آسیب‌پذیری دور زدن فرایند احراز هویت مانند CVE-2020-29015 ترکیب شده و کار را برای مهاجم آسان کند.

مهاجمان به محض احرازهویت شدن در رابط مدیریت دستگاه FortiWeb قادر خواهند بود دستورات دلخواه خود را با استفاده از backticks در فیلد "Name" در صفحه پیکربندی SAML Server اجرا نمایند. این دستورات به عنوان کاربر root در سیستم‌عامل اجرا خواهند شد.

مهاجم می‌تواند از این آسیب‌پذیری برای کنترل کامل دستگاه آسیب‌پذیر با بالاترین سطح دسترسی ممکن استفاده کند. مهاجم ممکن است یک shell دائمی، یک نرم‌افزار استخراج رمزارز یا سایر نرم‌افزارهای مخرب را در دستگاه آسیب‌پذیر نصب کند.

اگر رابط مدیریت این دستگاه از طریق اینترنت در دسترس باشد آسیب می‌تواند بدتر و خطرناک‌تر باشد. Rapid7 خاطرنشان کرد که در این صورت مهاجمان به شبکه گسترده‌تری دسترسی دارند. با این حال، محققان Rapid7 تاکنون ۳۰۰ دستگاه را شناسایی کرده‌اند که رابط مدیریت آن‌ها از طریق اینترنت در دسترس است.

در این تجزیه و تحلیل‌ها، Vu یک کد اثبات مفهومی (PoC) ارائه نمود که از درخواست و پاسخ HTTP POST استفاده می‌کند. با توجه افشای این خبر، Fortinet که قصد داشت این نقص را در پایان ماه آگوست در نسخه ۶.۴.۱ برطرف کند، این اقدام را در اولویت قرار داده و احتمالاً تا پایان این هفته نسخه‌ی به‌روزشده‌ی آن در دسترس خواهد بود.

محققان Rapid7 می‌گویند به نظر می‌رسد این آسیب‌پذیری مربوط به CVE-2021-22123 باشد که در ماه ژوئن وصله شد.

توصیه امنیتی:

Rapid7 به کاربران توصیه می‌کند تا زمان انتشار نسخه‌ی به‌روزشده، کاربران رابط مدیریت دستگاه FortiWeb را برای شبکه‌های غیرقابل اعتماد که اینترنت را هم می‌تواند شامل شود غیرفعال کنند. البته به طور کلی، رابط‌های مدیریت دستگاه‌هایی مانند FortiWeb به هر حال نباید مستقیماً از طریق اینترنت در دسترس باشند- رابط مدیریت این دستگاه‌ها فقط باید از طریق شبکه‌های داخلی قابل اعتماد یا از طریق اتصال VPN امن قابل دسترسی باشند.

منبع خبر :

Scan Link

آسیب‌پذیری XSS در افزونه SEOPress وردپرس امکان تسخیر سایت را فراهم می‌کند

این آسیب‌پذیری می‌تواند موجب اقدامات مخربی از جمله تسخیر سایت شود. این افزونه ی آسیب‌پذیر بر روی ۱۰۰،۰۰۰ وب‌سایت نصب شده است.

به گفته‌ی محققان، آسیب‌پذیری stored cross-site scripting (XSS) در افزونه‌ی SEOPress، به مهاجمان اجازه می‌دهد اسکریپت‌های وب دلخواه خود را به وب‌سایت‌ها تزریق کنند.

SEOPress یک ابزار بهینه‌سازی موتورهای جستجو (SEO) است که امکان مدیریت متادیتای SEO، کارت‌های social-media، تنظیمات Google Ad و سایر موارد را به مدیران سایت می‌دهد. محققان Wordfence در یک پست وبلاگی در روز دوشنبه گفتند: "یکی از ویژگی‌های این افزونه امکان افزودن عنوان SEO و توضیحات به پست‌ها است و این می‌تواند هنگام ذخیره‌ی ویرایش‌ها در یک پست یا از طریق REST-APIهای اخیراً معرفی‌شده انجام شود."متأسفانه این REST-API endpoint به صورت ناامن

پیاده‌سازی شده است.

این آسیب‌پذیری با شناسه‌ی CVE-2021-34641، به هر کاربر احراز هویت‌شده‌ای اجازه می‌دهد مانند یکی از مشترکان سایت، REST route را با یک nonce معتبر فراخوانی کند و عنوان و توضیحات SEO را برای هر پست تغییر دهد.

به گفته‌ی این پست: "مجوزهای فراخوانی برای endpoint فقط در صورتی تأیید می‌شود که کاربر یک REST-API nonce معتبر در درخواست داشته باشد." یک REST-API nonce معتبر می‌تواند توسط هر کاربر احراز هویت‌شده‌ای با استفاده از rest-nonce WordPress core AJAX action تولید شود.

به گفته‌ی محققان، بسته به اینکه مهاجم عنوان و توضیحات پست را به چه چیزی تغییر می‌دهد، اقدامات مخرب مختلفی را تا تسخیر سایت می‌تواند منجر شود. به دلیل عدم تفکیک و بررسی پارامترهای ذخیره‌شده، پی‌لود می‌تواند شامل اسکریپت‌های وب مخرب مانند جاوااسکریپت باشد. این اسکریپت‌ها هر بار که کاربر به صفحه‌ی "تمام نوشته‌ها" دسترسی یابد اجرا می‌شود. آسیب‌پذیری‌های cross-site scripting مانند این آسیب‌پذیری می‌توانند منجر به اقدامات مخرب مختلفی مانند ایجاد حساب کاربری جدید با دسترسی ادمین، تزریق webshell، ریدایرکت‌های دلخواه و اقدامات دیگر شود. این آسیب‌پذیری به راحتی می‌تواند توسط مهاجم برای تصاحب یک سایت وردپرسی مورد سوءاستفاده قرار گیرد.

توصیه امنیتی:

به منظور محافظت از وب‌سایت‌های وردپرسی خود در برابر خطرات ناشی از این آسیب پذیری، به کاربران توصیه می‌شود افزونه‌ی SEOPress را به نسخه‌ی ۵.۰.۴ به‌روزرسانی کنند.

منبع خبر :

Scan Link

اخبار کوتاه

۱۰ راه حل فیلترینگ DNS برای محافظت در برابر حملات سایبری

حملات سایبری در همه جای جهان اتفاق می افتد، بنابراین شما نه تنها باید شرکت خود را حفظ کنید، بلکه باید کارمندان و اعضای تیم خود را نیز نجات دهید. برای مقابله با حملات هکری، فیلتر کردن DNS یک راه‌حل عالی برای دریافت دروازه وب می باشد.

شاید برای شما این سؤال پیش آمده باشد که فیلتر DNS چیست؟ فیلتر DNS روشی است که دسترسی وب‌سایت ، آدرس IP و صفحات وب خاص را مسدود می‌کند. این کار مانند دفترچه تلفن اینترنتی است که در آن شما فقط باید نام دامنه سایت را وارد کرده و به آن دسترسی داشته باشید. این روند دسترسی شما را راحت‌تر می کند.

هنگام وارد کردن نام دامنه فیلتر DNS در ابتدا آدرس IP را از شما می پرسد و سپس شما را به سایت هدایت می کند. این کار یک شبکه امن را تضمین می کند که امکان کنترل بیشتر برای دسترسی به اینترنت را فراهم می کند و از حملات سایبری را مصون نگه داشته و بهره‌وری بهتری را به شما می‌دهد. فیلتر DNS باعث می شود ترافیک وب شما (ورودی و خروجی) مورد ارزیابی قرار گرفته و فقط ترافیک ایمن وارد شبکه شود.

این فرایند فیلترینگ را می‌توان در هر سایت طبقه‌بندی‌شده مانند سایت رسانه‌های اجتماعی، اخبار، سایت غیرقانونی، سایت نامناسب، کمپین‌های فیشینگ ، سایت مخرب و غیره انجام داد. با توجه به این وضعیت بیماری همه‌گیر کرونا که موجب افزایش آمار کار در خانه گردیده است، برای حفظ امنیت در کسب و کار شما چندین روش محافظت فیلتر DNS داریم.

۱۰ روش برتر محافظت از حملات سایبری که فیلتر DNS به ارمغان می‌آورد:

۱. Open DNS

۲. Cloudflare Gateway

۳. DNSFilter

۴. SafeDNS

۵. Webroot

۶. DNSCyte

۷. Cisco Umbrella

۸. CIRA DNS Firewall

۹. MXToolbox

۱۰. ScoutDNS

نقش کمپین "نه به باج‌افزار" در بازیابی اطلاعات ٦ میلیون قربانی باج‌افزار

کمپین "نه به باج افزار"، به بیش از ۶ میلیون قربانی کمک کرده است تا فایل‌هایی را که تحت حمله باج افزار قرار گرفته‌اند؛ بازیابی کنند. نه به باج افزار (NMR) خلاقیتی است که توسط مرکز جرایم رایانه‌ای اروپا یوروپ، واحد ملی جرایم پیشرفته فناوری پلیس و مک آفی ایجاد شده است و به قربانیان باج‌افزار کمک می‌کند تا داده‌های رمزگذاری شده را بدون پرداخت هزینه به مجرمان، بازیابی کنند. این برنامه در پنج سال حیات خود روند از پرداخت یک بیلیون یورو به مجرمان جلوگیری کرده است.

باج افزار، مجرمان را قادر می‌سازد تا تمام اطلاعات دیجیتالی ذخیره شده را سرقت کنند. این نوع حمله مخرب بسیار گسترده شده است و به کاربران و سازمان‌های خصوصی در سراسر جهان آسیب زیادی وارد کرده است. این اقدامات برای آگاهی سازی و محافظت از دنیای دیجیتال می‌باشد. ابزارهای رمزگشایی، پس از بارگیری و راه‌اندازی، به قربانیان باج‌افزارها کمک می‌کنند تا داده‌های خود را بدون پرداخت هزینه‌ای پس بگیرند. این وب سایت همچنین شامل توصیه‌های پیشگیرانه ودستورالعمل‌ها در مورد نحوه‌ی گزارش جرایم سایبری در یک کشور به‌خصوص است.طبق پست منتشر شده توسط یوروپل، مخزن نه به باج افزار، به بیش از شش میلیون نفر کمک کرده است تا اطلاعات خود را به صورت رایگان بازیابی کنند. همین امر مانع از کسب درآمد یک بیلیون یورویی مجرمان از طریق حملات سایبری شد. این پورتال به ۳۷ زبان در دسترس است.

مقالات آموزشی

روش‌های ایمن‌سازی زیرساخت اکتیودایرکتوری (بخش دوم)

در ادامه‌ی مبحث ایمن‌سازی زیرساخت اکتیودایرکتوری که بخش اول آن در بولتن شماره ۳۰ مطرح شد، ادامه‌ی موارد به صورت زیر می‌باشد:

۱۳- کمینه‌سازی سرویس‌های غیرضروری و پورت‌های باز

علاوه بر بستن پورت‌های غیرضروری اقداماتی نیز باید در جهت جلوگیری از حملات DoS بر روی کنترل‌کننده‌های دامنه (DC) اعمال گردد. روش‌های زیادی موجود است تا کنترل‌کننده دامنه (DC) را مورد حمله DoS قرار دهد و از دور خارج کند. یکی از این روش‌ها پر کردن فضای دیسک کنترل‌کننده دامنه (DC) است. این روش با ساخت پی در پی اشیا در اکتیودایرکتوری و بالابردن حجم NTDS.DIT انجام می‌شود. علاوه بر اینکه فایل NTDS.DIT باید در پارتیشنی قرار گیرد که فضای خالی زیادی داشته باشد، باید با استفاده از دستورات DSMOD PARTITION و DSMOD QUOTA میزان رشد پایگاه داده را تعریف نماییم تا از ایجاد بی‌رویه اشیا در اکتیودایرکتوری جلوگیری نماییم. یکی دیگر از حملات DoS که بر روی کنترل‌کننده دامنه (DC) انجام می‌پذیرد، ارسال سیل فایل (File Flooding) به پوشه SYSVOL می‌باشد که باعث از کار افتادگی کنترل‌کننده دامنه (DC) خواهد شد. در این مورد خاص امکان تعریف Quota وجود ندارد اما می‌توان با تعریف نمودن مقداری از فضای پوشه SYSVOL به عنوان فضای رزرو مانع از بوجود آمدن این مشکل شد. در صورت بوجود آمدن مشکل و پر شدن فضای دیسک می‌توان فضای رزرو شده را پاک کرد تا فضای خالی ایجاد گردد. این امکان با استفاده از دستور FSUTIL FILE CREATENEW انجام می‌شود.

۱۴- امن نمودن منبع زمان کنترل‌کننده دامنه (DC)

به‌دلیل وابستگی شدید سرویس اکتیودایرکتوری به پروتکل Kerberos ، این سرویس به شدت به اختلاف زمان حساس می‌باشد. به صورت پیش‌فرض کنترل‌کننده دامنه (DC) موجود در ریشه اصلی Forest مسئولیت همسان‌سازی زمان سایر کنترل‌کننده‌های دامنه (DC) را بر عهده دارد. این بدین معنی است که سایر کنترل کننده‌های دامنه (DC) ها زمان خود را با کنترل‌کننده دامنه (DC) اصلی موجود در ریشه تنظیم می‌کنند تا از عدم

اختلاف زمانی در ساختار جلوگیری شود. باید در نظر داشت، حال که کنترل‌کننده دامنه (DC) موجود در ریشه Forest به عنوان منبع اصلی زمان در کل ساختار به ایفای نقش می‌پردازد، زمان خود را با یک منبع خارج از سازمان تنظیم می‌نماید. آیا این منبع زمانی که در خارج از سازمان قرار دارد امن است؟

۱۵- ممیزی رخدادهای مهم

باید قابلیت ممیزی (Audit) رخدادهای مهم را در سطح دامنه فعال کرده تا امکان ثبت آن رخدادها برای تمام سیستم‌ها به وجود آید. پیشنهاد می‌شود ثبت رخدادهای مرتبط با احراز هویت‌های ناموفق و موفق، دسترسی به فایل‌ها و پوشه‌های حساس و تغییرات GPO تنظیم گردد.

۱۶- استفاده از IPSec

پیاده‌سازی IPSec برای ارتباطات بین کلاینت و کنترل‌کننده دامنه (DC) اگرچه کار پیچیده‌ای بوده و نیازمند صرف زمان قابل توجهی می‌باشد، امکان پیاده‌سازی آن برای ارتباطات بین کنترل‌کننده دامنه (DC) به میزان قابل توجهی آسان‌تر می‌باشد. از این پروتکل برای ارتباطات بین کنترل‌کننده‌های دامنه (DC) استفاده نمایید.

۱۷- ذخیره نکردن مقادیر Hash پروتکل LAN Manager

با توجه به قدیمی بودن پروتکل LM و ساختار ضعیف آن، باید هرچه سریع‌تر ساختار خود را از این ضعف امنیتی رها کنید. بسیاری از حملات مرتبط به رمز عبور با حمله به Hash این پروتکل شروع شده و با استنتاج نتایج به‌دست آمده به پروتکل‌های دیگری مانند NTLM حمله می‌نمایند. سیاست امنیتی که باید در این سناریو مورد بازبینی قرار گیرد Do Not Store LAN Manager Hash Value on Next Password Change می‌باشد. همچنین سیاست امنیتی دیگری که باید مورد توجه قرار گیرد سیاست Send NTLMv2 Response Only, Refuse LM and NTLM است. اکثر کلاینت‌ها می‌توانند تنظیم گردند تا از NTLMv2 به عنوان پروتکل اصلی استفاده نمایند، اگرچه پیاده‌سازی این سیاست‌های امنیتی نیاز به تست در محیط آزمایشی و اطمینان حاصل نمودن از صحت عملکرد آن‌ها می‌باشد.

۱۸- مدیریت وصله‌های ترمیمی

بسیاری از حملاتی که به سرویس‌های یک سازمان انجام می‌شود به‌دلیل به‌روز نبودن آن سرویس از وصله‌های ترمیمی می‌باشد. سازمان‌های کوچک از ابزار WSUS برای مدیریت و گسترش دادن وصله‌های ترمیمی و سازمان‌های بزرگ از نرم‌افزارهای مدیریتی مثل SCCM برای این منظور استفاده می‌کنند. بدون توجه به مکانیزمی که برای گسترش وصله‌های ترمیمی به سرورها و ایستگاهای کاری استفاده می‌شود، باید آن‌ها را برای سیستم‌های با امنیت بالا مانند کنترل کننده‌های دامنه جدا کنید.

۱۹- عدم دسترسی به اینترنت برای سرویس‌های حساس

به‌دلیل اینکه اکثر حملاتی که به سازمان صورت می‌پذیرد از نقاطی خارج از سازمان انجام می‌شود، می‌توان نتیجه گرفت که اینترنت دروازه حملات به داخل سازمان می‌باشد. برای رفع این مشکل امنیتی بهتر است که دسترسی به اینترنت را برای سیستم‌های حساس محدود نمایید. دلیل قابل توجیهی برای اینکه کنترل کننده‌های دامنه به اینترنت متصل باشند وجود ندارد.

۲۰- تمهیدات لازم جهت ایمن‌سازی میزبان‌های مدیریتی (Administrative Hosts)

پیشنهاد می‌شود میزبان‌هایی که دارای بار عملیاتی و مدیریتی حساس هستند برای احراز هویت کاربران، علاوه بر رمز عبور از تکنولوژی‌های دیگری مانند Smartcard استفاده نمایند. همچنین می‌توان از طریق پیاده‌سازی سیاست‌های امنیتی (GPO) مشخص کرد که چه کسانی قادر به استفاده از آن سیستم به صورت محاوره‌ای (Interactive) هستند تا مانع دسترسی افراد غیر مجاز به آن میزبان گردد.

۲۱- محدود نمودن نرم‌افزارهای اجرایی بر روی کنترل‌کننده‌های دامنه با استفاده از Applocker

قابلیت Applocker یک کنترل‌کننده نرم‌افزارهای اجرایی بر روی ویندوز می‌باشد که به صورت پیش‌فرض نصب شده ولی غیرفعال می‌باشد. این قابلیت به مدیران اجازه می‌دهد که لیستی موسوم به "لیست سفید" تهیه کرده که در آن نرم‌افزارهایی که مجاز به اجرا بر روی کنترل‌کننده‌های دامنه هستند تعریف می‌گردند و هرگونه نرم‌افزار که خارج از لیست فوق باشد اجازه اجرا نخواهد داشت. پس از پیاده‌سازی کامل کنترل‌کننده‌های دامنه و نصب نرم‌افزارهای مورد نیاز از قبیل نرم‌افزارهای امنیتی ضدویروس، نرم‌افزارهای مانیتورینگ و سایر نرم‌افزارها، پیشنهاد می‌شود که لیستی از نرم‌افزارهای نصب‌شده تهیه کرده و آن را به Applocker ارائه دهید. در این‌صورت در شرایطی که دسترسی غیرمجاز به هر نحوی بر روی کنترلرهای دامنه انجام گیرد، شخص مهاجم اجازه نصب و اجرای نرم‌افزارهای خارج از لیست را نخواهد داشت.

۲۲- اعطای سطح دسترسی برحسب روش‌هایی مانند RBAC

پیشنهاد می‌شود راهبرانی که در سطح دامنه مشغول فعالیت هستند را با توجه به موقعیت شغلی آن‌ها دسته‌بندی کرده و دسترسی‌های لازم را بر اساس موقعیت شغلی به آن‌ها اعمال نماییم. به عنوان مثال، مدیرانی که وظیفه مدیریت نام‌های کاربری و رمز عبور را بر عهده دارند را در گروهی به نام Account_Admins قرار داده و سطوح دسترسی مورد نیاز را با استفاده از تکنیک Delegation به آن گروه اعمال نمایید.

اخبار کوتاه

هشدار مایکروسافت در مورد بدافزار LemonDuck

مایکروسافت به مشتریان درباره بدافزار رمزنگاری LemonDuck که سیستم‌های ویندوز و لینوکس را هدف قرار می‌دهد هشدار داد. این بدافزار از طریق ایمیل، اکسپلویت، دستگاه‌های USB، حملات بی‌رحمانه، و همچنین حملاتی که در ماه مارس از آسیب‌پذیری‌های حیاتی بازار بورس اوراق بهادار استفاده کرد، گسترش می‌یابد.

قابل ذکر است، گروه پشت LemonDuck از اشکالات امنیتی برجسته استفاده می‌کند و آسیب‌پذیری‌های قدیمی‌تر که در طول دوره‌هایی که تیم‌های امنیتی بر رفع اشکالات مهم و حتی حذف بدافزارهای رقیب متمرکز هستند، بکار می‌گیرد.

مایکروسافت خاطرنشان کرد: "[LemonDuck] همچنان از آسیب‌پذیری‌های قدیمی‌تر استفاده می‌کند، و زمان‌هایی که متمرکز بر وصله کردن یک آسیب‌پذیری عمومی به جای بررسی سازش است، به نفع مهاجمان عمل می‌کند."

اخبار داخلی

پارســـو راهـــکار منتـــخب در حـــوزه هویت دیجـــیتال

پارسو (Parsso) _محصول شرکت دانش‌بنیان رادپرداز رازی_ یک سامانه احراز هویت متمرکز و جامع جهت ارائه خدمات single sign-on (SSO) می‌باشد. این سامانه از تمامی پروتکل‌های رایج و استاندارد احراز هویت از جمله OAuth، SAML، CAS و OpenID و نیز از زبان‌های برنامه‌نویسی رایج پشتیبانی کرده و قابلیت اتصال به تمامی محصولات CMS را دارا می‌باشد. از برتری‌های این محصول می‌توان به پیاده‌سازی احراز هویت دو مرحله‌ای، احراز هویت مبتنی بر ویژگی‌های بیومتریک، احراز هویت با استفاده از توکن سخت‌افزاری و واسط کاربری ساده با پشتیبانی همزمان از زبان‌های فارسی و انگلیسی اشاره کرد. با این سامانه، مدیریت حساب‌های کاربری، سیاست‌های امنیتی رمزهای عبور، کنترل و پیگیری عملیات احراز هویت به صورت متمرکز فراهم می‌شود.

شرکت راهبران هویت مجازی آینده (برهان) برای اولین بار در کشور اقدام به شناسایی راهکارهای ایرانی تأثیرگذار بر زیست‌بوم هویت دیجیتال کشور کرده است و نقشه جامع این راهکارها را مطابق تصویر زیر در ۷ خوشه بر اساس کارکرد آن‌ها به تصویر کشیده است.

مفتخریم تا به اطلاع شما برسانیم محصول شرکت رادپرداز رازی (یک شرکت دانش‌بنیان منشعب شده از مرکز آپا دانشگاه رازی) با نام سامانه احراز هویت متمرکز پارسو پس از بررسی اولیه به عنوان راهکار منتخب شناسایی شده و جزء ۶۰ راهکار برتر کشور در حوزه هویت دیجیتال در بخش «مدیریت هویت و دسترسی» قرار گرفته است.

تصویر بعد جایگاه پارسو را در بخش مدیریت و دسترسی به عنوان یکی از راهکارهای منتخب نشان می‌دهد.

اخبار کوتاه

کلاهبرداران از مراکز تماس جعلی برای انتشار باج افزار استفاده می‌کنند

در BazaCall، از روش شبیه به "vishing" استفاده می‌شود که در آن قربانیان پیام‌هایی را دریافت می‌کنند که به آن‌ها اطلاع می‌دهد اگر با شماره تلفن خاصی تماس نگیرند، اشتراک آن‌ها به پایان می‌رسد یا هزینه اشتراک اعمال می‌شود.

کمپین جدیدی مشخص شد که در آن مراکز تماس جعلی قربانیان را فریب می‌دهند تا بدافزارها را بارگیری کرده، داده‌ها را حذف کرده و باج‌افزارها را در دستگاه آسیب‌پذیر مستقر کنند. این حمله BazaCall نام دارد.

این کمپین جدید توسط تیم اطلاعاتی Microsoft 365 Defender Threat Intelligence کشف و گزارش شد. محققان خاطرنشان کردند که حملات BazaCall می‌تواند به سرعت در یک شبکه گسترش یابد و اعتبار و سرقت گسترده اطلاعات را انجام دهد. همچنین می‌تواند باج افزار را تنها در ۴۸ ساعت پس از سازش توزیع کند.

به نظر می‌رسد این کمپین از روندی الهام گرفته‌شده است که جنایتکاران مرتبط با BazaLoader از مراکز تماس، عمدتاً درجایی که انگلیسی‌زبانان غیربومی در آن استفاده می‌کنند، در زنجیره حملات پیچیده خود استفاده می‌کنند.

چگونه BazaCall قربانیان را به دام می‌اندازد؟

از شیوه‌های سنتی مهندسی اجتماعی که ما به آن عادت کرده‌ایم، مانند مواردی که URLهای سرکش یا اسناد آلوده برای انتشار بدافزار استفاده می‌شود، دوری می‌کند. در BazaCall، از روش "vishing-like" استفاده می‌شود. در این حمله، قربانیان پیام‌هایی از طریق ایمیل دریافت می‌کنند که به آن‌ها اطلاع می‌دهد هزینه اشتراک اعمال می‌شود یا اگر با شماره تلفن خاصی تماس نگیرند، اشتراک آن‌ها به پایان می‌رسد. وقتی قربانی با آن شماره تماس می‌گیرد، با کارمندی در مرکز تماس جعلی ارتباط برقرار می‌کند که به او دستور می‌دهد از یک وب‌سایت با ظاهر واقعی دیدن کند. قربانی باید یک فایل را از صفحه حساب خودبارگیری کند تا اشتراک را لغو کند. پس از فعال شدن ماکروها بر روی اسناد بارگیری شده، بدافزار BazaLoader از یک فانوس دریایی Cobalt Strike تحویل داده می‌شود. BazaLoader همچنین بانام BazarBackdoor شناخته می‌شود، یک بارگیری مبتنی بر C ++ است. شبکه‌های Palo Alto برای اولین بار این بدافزار را در مارس ۲۰۲۱ کشف کردند. این نرم‌افزار می‌تواند انواع مختلف نرم‌افزارهای مخرب را روی ماشین‌های آلوده نصب کند، ازجمله باج افزار و بدافزار سرقت اطلاعات.

ثبت‌نام دوره‌های آنلاین مرکز آپا دانشگاه رازی

دوره امنیت شبکه سیسکو
CCNA Security

دوره حرفه‌ای شبکه سیسکو
CCNP Enterprise Core
ENCOR 350-401

دوره هکر قانونمند
CEH v11

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-1400

<راه‌های ارتباطی>

cert.razi.ac.ir
۰۸۳۳۴۳۴۳۲۵۱
APARazi
APA_Razi


مرکز تخصصی آپا دانشگاه رازی