بسمه تعالی

حذف دسترسی‌های admin و تأثیر آن بر آسیب‌پذیری‌های موجود در محصولات مایکروسافت

گزارش فنی

شناسه سند ..... TR_ MicrosoftVulnerabilities_13990230

نوع سند ..... گزارش فنی

شماره نگارش ۱/۰

تاریخ نگارش ۱۳۹۹/۰۲/۳۰

طبقه‌بندی سند ..... **عادی**

شاهرود، میدان هفت تیر، بلوار دانشگاه، دانشگاه صنعتی شاهرود، مرکز تخصصی آپا، کد پستی: ۳۶۱۹۹۹۵۱۶۱

(۰۲۳) ۲۲۰۴-۳۲۳۹ (۰۲۳) ۰۲۵۱-۳۲۳۰ cert.shahroodut.ac.ir

فهرست مطالب

فهرست شکل‌ها

۱ مقدمه

با وجود هشدارهای مداوم، سازمان‌ها از حساب‌های کاربری با امتیاز بالا محافظت نمی‌کنند. این حساب‌ها، هدف اولیه‌ی مجرمان سایبری و مهاجمان هستند. اگر دسترسی به این حساب‌ها ممکن باشد، ممکن است سازمان با خطر بسیار جدی مواجه شود. با این وجود، مدیریت این حساب‌های حساس هنوز به صورت صحیحی انجام نمی‌شود.

از آنجا که مخاطرات امنیتی اجتناب‌ناپذیر هستند، تنها راه کاستن از آن‌ها حذف امتیازات مدیر سیستم برای کاربران معمولی و تخصیص آن‌ها تنها در هنگام نیاز و در یک بازه زمانی محدود است. کاهش دسترسی‌های غیرضروری مدیران سیستم (admin) علاوه بر کاهش مخاطرات داخلی، منجر به افزایش امنیت در برابر تهدیدهای بیرونی نیز می‌شود.

در این گزارش به بررسی آسیب‌پذیری‌های مایکروسافت در محصولات مختلف این شرکت می‌پردازیم، دید جامعی از روندهای مرتبط به آسیب‌پذیری را ارائه داده و از همه مهم‌تر این که چه تعداد از آسیب‌پذیری‌ها در صورت حذف امتیازات admin از سازمان‌ها کاهش داده شده‌اند، بررسی می‌شود. با حذف دسترسی‌های admin از حساب‌های کاربری می‌توان با اغلب آسیب‌پذیری‌های بحرانی شناخته شده در محصولات مایکروسافت مقابله کرد؛ که وجود این آسیب‌پذیری‌ها به معنای بد یا ناامن بودن محصولات مایکروسافت نیست.

۲ تاثیرپذیری حذف دسترسی admin

حذف یا غیرفعال سازی دسترسی‌های غیرضروری مدیر سیستم، منجر به از بین رفتن کامل مخاطرات درون سازمانی نمی‌شود، بلکه می‌توان تمام فعالیت‌ها را تحت کنترل خود گرفت.

یک کاربر حتی بدون در اختیار داشتن دسترسی admin می‌تواند به صورت عمدی یا غیرعمدی، فعالیت‌های مخربی را انجام دهد؛ از جمله:

- انتخاب یک کلمه عبور ضعیف
- استفاده از کلمه عبوری که از آن برای حساب‌های کاربری شخصی استفاده می‌کند.
- قرار دادن کلمه عبور خود در اختیار دیگران، که ممکن است از آن برای انجام اهداف خراب‌کارانه استفاده شود.
- کلیک بر روی لینک‌های ناامن موجود در ایمیل‌ها یا در اینترنت

- قرار دادن اطلاعات حساس و طبقه بندی شده در اختیار سایر اشخاص، در اثر کلاه‌برداری (مثل جعل هویت admin) یا به صورت غیرعمدی
- جاسوسی در فایل‌های رایانه‌ی یکی از همکاران، وقتی رایانه او بدون نظارت رها شده است (که بسیار خطرناک می‌باشد، به خصوص اگر این همکار به داده‌های مهم سازمانی دسترسی داشته باشد).
- اتصال یک درایو USB یا هارد اکسترنال آلوده به سیستم رایانه سازمانی

حذف دسترسی admin، در اغلب اوقات تأثیر چشم‌گیری بر کاهش مخاطرات داخلی دارد.

اگر کاربری به تمام امتیازات مدیر سیستم دسترسی کامل داشته باشد، قادر خواهد بود آسیب بسیاری به سازمان وارد کند. برخی از این آسیب‌ها عبارتند از:

- نصب نرم‌افزارهای مخربی همچون جاسوس‌افزار یا بدافزار برای سرقت پول، داده‌ها یا ایجاد اختلال در عملکرد سازمان
- ایجاد back door برای اشخاص دیگر، به منظور نصب نرم‌افزارهای مخرب یا نفوذ به سیستم‌ها
- دسترسی به اطلاعات حساس یا استخراج آن‌ها از شبکه، برای سوءاستفاده‌های بعدی
- اعمال تغییراتی جهت حذف دسترسی کاربران مجاز به سیستم‌ها

هکرها می‌توانند این اعمال مخرب را از طریق فریب کاربرانی که امتیازات سطح بالایی مانند مدیر سیستم دارند، انجام دهند. این ترفند را می‌توان به روش‌های مختلفی اجرا کرد: ارسال ایمیل هرزنامه، عوض کردن یک USB با USB متعلق به هکر و غیره.

۳ خلاصه آمار آسیب‌پذیری‌های مایکروسافت

۱) در سال ۲۰۱۹ تعداد ۸۵۸ آسیب‌پذیری مایکروسافت کشف شده‌اند.
۲) تعداد آسیب‌پذیری‌های گزارش شده، ٪۶۴ نسبت به ۵ سال گذشته افزایش یافته است. (۲۰۱۹-۲۰۱۵)
۳) حذف امتیازات admin، ٪۷۷ از کل آسیب‌پذیری‌های بحرانی مایکروسافت در سال ۲۰۱۹ را کاهش می‌دهد.
۴) کلیه آسیب‌پذیری‌های بحرانی در Internet Explorer و Edge با حذف امتیازات admin کاهش داده شده‌اند.
۵) کلیه آسیب‌پذیری‌های بحرانی که ویندوز ۷، ۸٫۱ و ۱۰ را تحت تأثیر قرار می‌دهند، با حذف امتیازات admin کاهش داده شده‌اند.

این موارد در شکل ۱ مشاهده می‌شود.

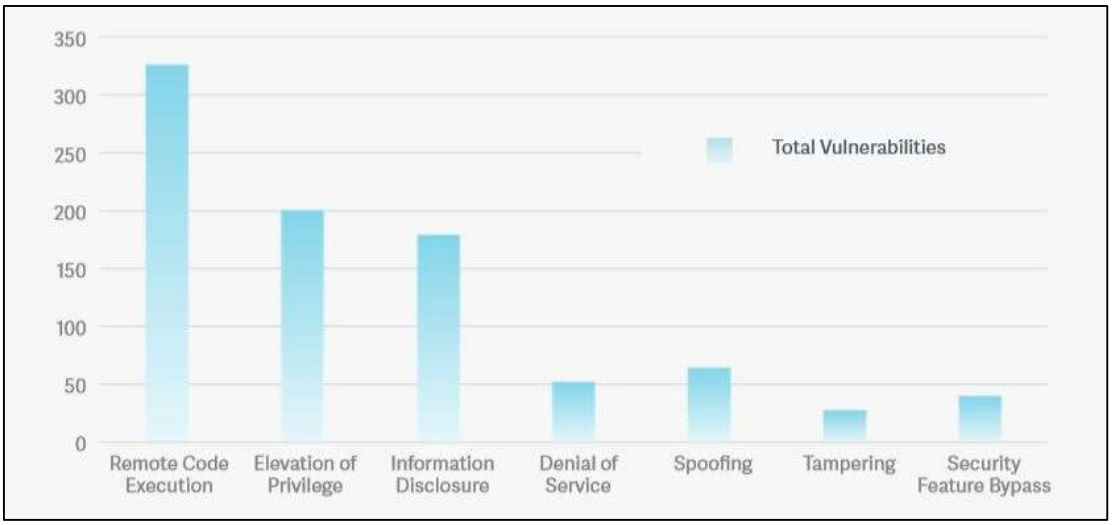
شکل ۱: خلاصه آمار آسیب‌پذیری‌ها

شکل ۲ درصد آسیب‌پذیری‌های کاهش یافته با حذف حقوق admin را نشان می‌دهد.

شکل ۲: درصد آسیب‌پذیری‌های کاهش یافته با حذف حقوق admin

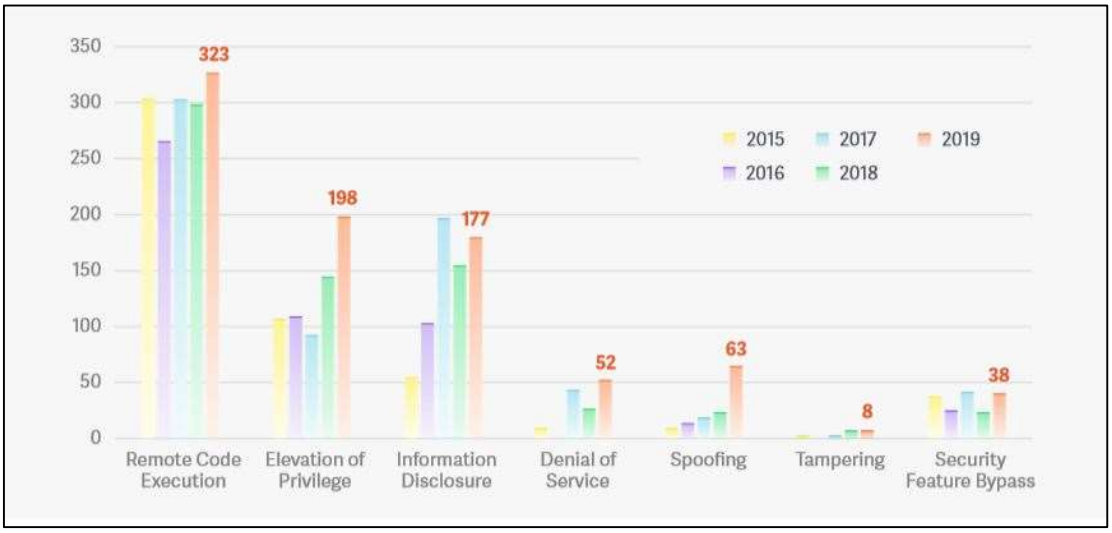
۴ آسیب‌پذیری‌ها چگونه در مایکروسافت طبقه‌بندی می‌شوند؟

هر بولتن امنیتی مایکروسافت شامل توصیف یک یا تعداد بیشتری آسیب‌پذیری است که بر چندین محصول اثر می‌گذارد. این موارد طبق نوع تأثیر، که شامل اجرای کد از راه دور، افزایش دسترسی‌ها، افشای اطلاعات، انکار سرویس، دور زدن ویژگی امنیتی، کلاه‌برداری و مداخله می‌باشد، طبقه‌بندی می‌شوند. شکل ۳ میزان انواع مختلف آسیب‌پذیری‌های مایکروسافت در سال ۲۰۱۹ را نمایش می‌دهد.



شکل ۳: میزان انواع مختلف آسیب‌پذیری‌های مایکروسافت در سال ۲۰۱۹

همانند گزارش‌های سال‌های گذشته، آسیب‌پذیری اجرای کد از راه دور (RCE) در سال ۲۰۱۹ افزایش زیادی پیدا کرده است و بیشترین سهم از کل آسیب‌پذیری‌های مایکروسافت را تشکیل می‌دهد. از ۳۲۳ آسیب‌پذیری اجرای کد از راه دور، ۱۹۱ آسیب‌پذیری بحرانی در نظر گرفته شده‌اند. حذف امتیازات admin باعث کاهش ۷۶٪ از این آسیب‌پذیری‌های بحرانی شده است. همچنین میزان آسیب‌پذیری‌های افزایش دسترسی ۳۷٪ افزایش یافته است.



شکل ۴: میزان انواع مختلف آسیب‌پذیری‌ها (۲۰۱۹-۲۰۱۵)

۵ آسیب‌پذیری در محصولات مختلف مایکروسافت

۵-۱ Internet Explorer و EDGE

با وجود سلطه گوگل کروم و فایرفاکس، Internet Explorer هنوز هم یک مرورگر رایج است و مایکروسافت از ژانویه سال ۲۰۱۶ جدیدترین نسخه Internet Explorer را برای سیستم‌عامل‌های پشتیبانی شده، پشتیبانی و وصله می‌کند. شایان ذکر است که Internet Explorer (IE) نسخه ۱۰، از تاریخ ۳۱ ژانویه ۲۰۲۰ پشتیبانی نمی‌شود. از آن پس، IE ۱۱ به تنها نسخه پشتیبانی شده روی ویندوز سرور ۲۰۱۲ و ویندوز ۸ استاندارد تبدیل شد.

تعداد ۳۳ آسیب‌پذیری بحرانی در اینترنت اکسپلورر ۸، ۹، ۱۰ و ۱۱ طی سال ۲۰۱۹ یافت شد. حذف امتیازات admin، باعث کاهش صد درصد خطر این آسیب‌پذیری‌ها شد.

آسیب‌پذیری‌های بحرانی در مایکروسافت Edge از زمان شروع آن در دو سال پیش افزایش یافته و ۸۶ مورد آسیب‌پذیری بحرانی کشف شده است؛ حذف دسترسی‌های admin، صد درصد خطر این آسیب‌پذیری‌ها را کاهش داده است.

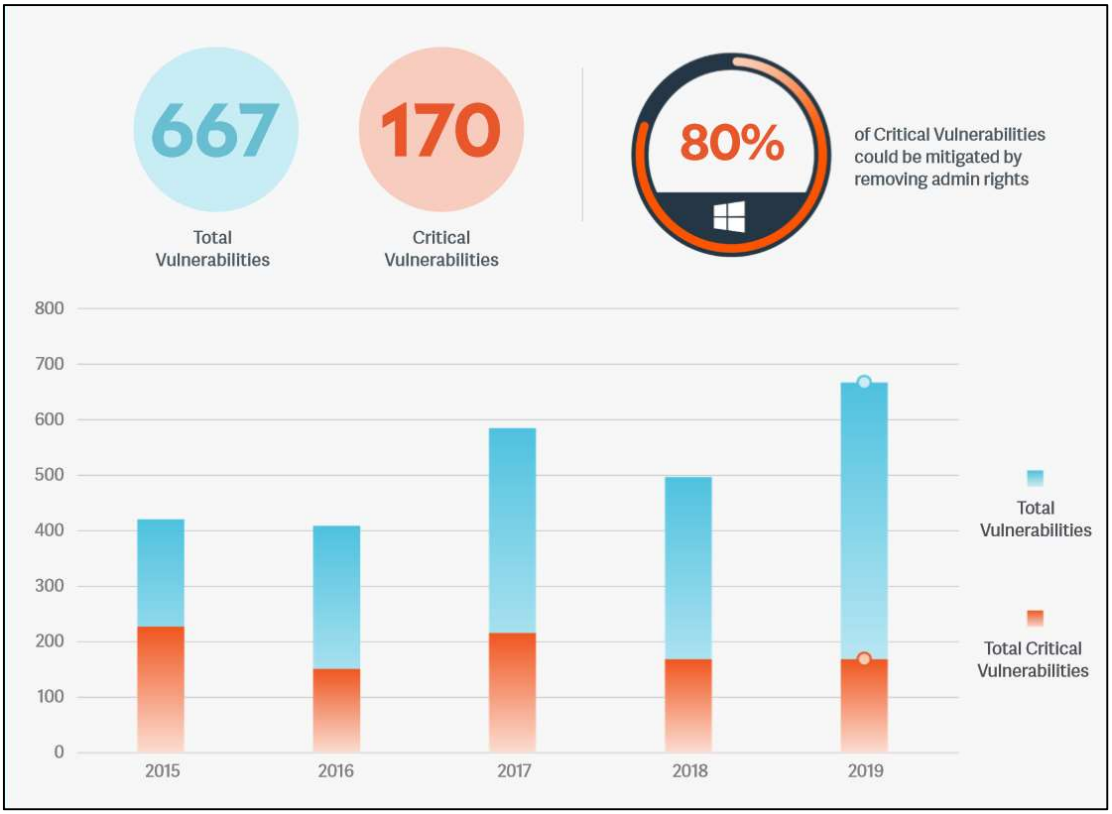
در ۱۵ ژانویه ۲۰۲۰، Edge به یک موتور مبتنی بر Chromium منتقل شد؛ در واقع کروم و Edge می‌توانند نقض‌های مشابهی داشته باشند؛ بنابراین هیچ مرورگری به اندازه کافی ایمن نیست تا از آن به عنوان یک استراتژی کاهش برای آسیب‌پذیری‌های Edge استفاده شود. شکل ۵ آسیب‌پذیری‌های Internet Explorer و Edge در سال‌های ۲۰۱۹-۲۰۱۵ را نمایش می‌دهد.

شکل ۵: آسیب‌پذیری‌های Internet Explorer و Edge در سال‌های ۲۰۱۹-۲۰۱۵

۵-۲ ویندوز

در سال ۲۰۱۹، ۶۶۷ آسیب‌پذیری در سیستم‌عامل‌های ویندوز Vista، ۷، RT، ۸/۸,۱ و ۱۰ گزارش شد. ویندوز ۱۰ به عنوان «امن‌ترین سیستم‌عامل ویندوز» تا به امروز عرضه شد؛ با این وجود در سال گذشته ۱۶۷ آسیب‌پذیری بحرانی در آن یافت شد. از بین آسیب‌پذیری‌های کشف شده ویندوز در سال ۲۰۱۹ ، ۱۷۰ مورد

بحرانی در نظر گرفته شدند. حذف امتیازات admin، ٪۸۰ درصد از این آسیب‌پذیری‌های بحرانی را کاهش داد. شکل ۶ آسیب‌پذیری‌های ویندوز در سال‌های ۲۰۱۹-۲۰۱۵ را نمایش می‌دهد.



شکل ۶: آسیب‌پذیری‌های ویندوز در سال‌های ۲۰۱۹-۲۰۱۵

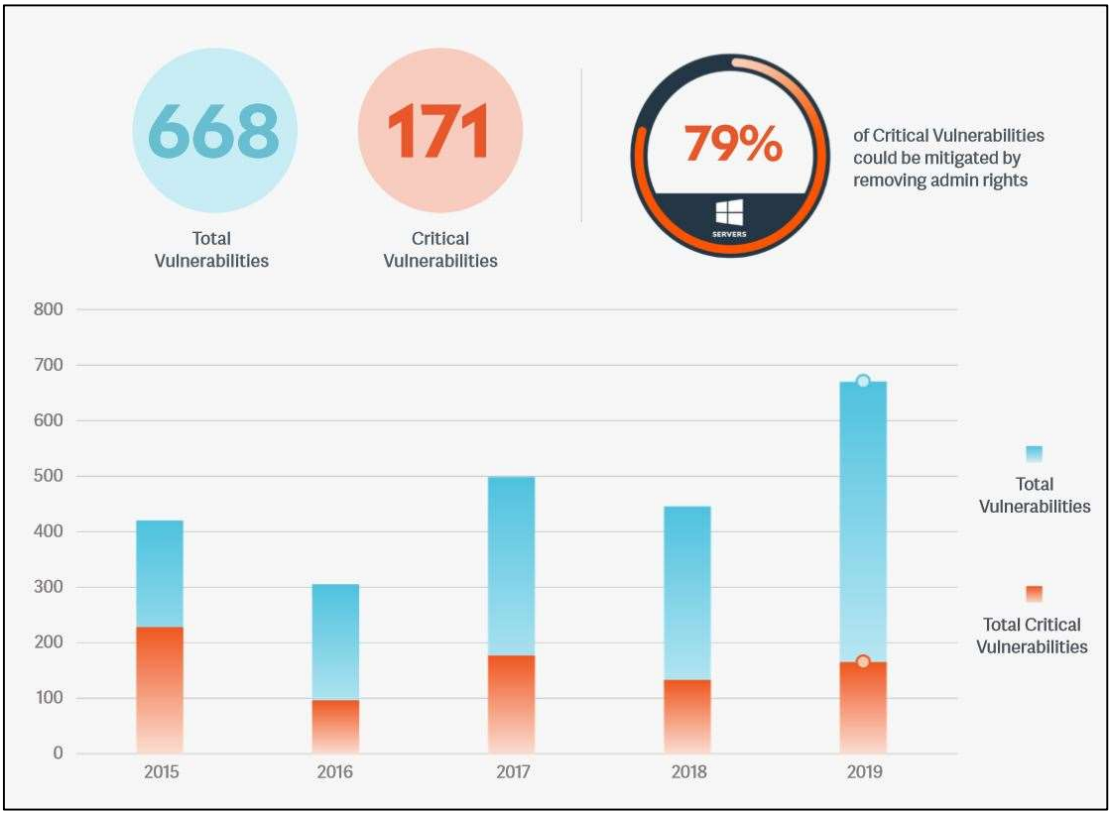
۵-۳ مایکروسافت آفیس

با توجه به میزان بالای آسیب‌پذیری‌ها (۱۰۲) در سال ۲۰۱۸، میزان آسیب‌پذیری‌های سال ۲۰۱۹ تقریباً نصف شد (۶۰)؛ که ۷ آسیب‌پذیری بحرانی گزارش شده و حذف امتیازات admin، باعث کاهش صد درصد آن‌ها در کلیه محصولات آفیس (ورد، اکسل، پاورپوینت، Visio، Publisher و غیره) شد. شکل ۷ نشان دهنده آسیب‌پذیری‌های مایکروسافت آفیس در سال‌های ۲۰۱۹-۲۰۱۵ می‌باشد.

شکل ۷: آسیب‌پذیری‌های مایکروسافت آفیس در سال‌های ۲۰۱۹-۲۰۱۵

۵-۴ ویندوز سرور

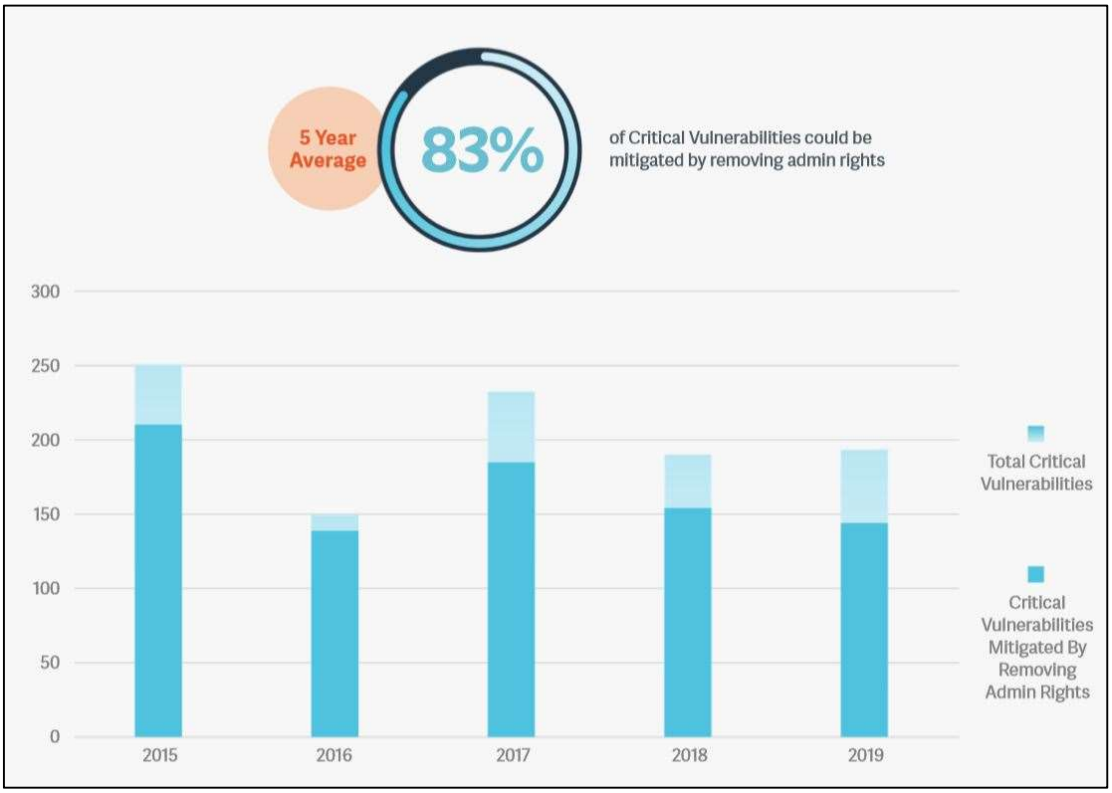
تعداد ۶۶۸ آسیب‌پذیری مربوط به ویندوز سرور در بولتن‌های امنیتی مایکروسافت در سال ۲۰۱۹ گزارش شد، که تعداد ۱۷۱ آسیب‌پذیری بحرانی تشخیص داده شده است؛ ٪۷۹ از این آسیب‌پذیری‌ها می‌توانند با حذف امتیازات admin کاهش یابند. شکل ۸ آسیب‌پذیری‌های ویندوز سرور را در سال‌های ۲۰۱۹-۲۰۱۵ نشان می‌دهد.



شکل ۸: آسیب‌پذیری‌های ویندوز سرور در سال‌های ۲۰۱۹-۲۰۱۵

در سال ۲۰۱۳، ۲۵۲ آسیب‌پذیری در مایکروسافت ویندوز سرور یافت شد که این به معنای افزایش قابل توجهی در آسیب‌پذیری‌های ۶ سال اخیر می‌باشد.

آسیب‌پذیری‌های بحرانی باعث تشخیص ریسک‌های سازمان شده و نگرانی‌های قابل توجهی برای سازمان‌های متعهد به محافظت از شبکه‌های خود و نقض داده‌ها ایجاد می‌کنند. تجزیه و تحلیل این گزارش تعیین می‌کند که بیشتر این آسیب‌پذیری‌ها می‌توانند با حذف دسترسی‌های admin محلی کاهش یابند. در **Error! Reference source not found.** آسیب‌پذیری‌های مایکروسافت با وجود امتیازات ادمین و پس از حذف آن نمایش داده شده است.



شکل ۹: آسیب‌پذیری‌های مایکروسافت در سال‌های ۲۰۱۹-۲۰۱۵

۶ نظرات تخصصی

در این بخش به بررسی برخی نظرات تخصصی محققان آزمایشگاه BeyondTrust در مورد حذف دسترسی‌های admin و تأثیر آن بر آسیب‌پذیری‌های ذکر شده می‌پردازیم. میزان داده‌های تولید شده و به اشتراک گذاشته شده به صورت تصاعدی در حال افزایش است و زیرساخت‌های امنیتی که از این داده‌ها محافظت می‌کنند، تحت فشار بیشتری قرار می‌گیرند. با افزایش حملات همراه با کمبود مهارت، کیفیت و حجم حملات نیز افزایش می‌یابد.

مهاجمانی که در جست‌وجوی نقاط ضعف هستند یا کارمندانی که به طور اتفاقی سازمان‌ها را از شیوه‌های ناامن به خطر می‌اندازند، به عنوان ضعیف‌ترین پیوند در نظر گرفته شده‌اند. به همین دلیل است که احتمالاً همه آسیب‌پذیری‌هایی که مورد بهره‌برداری قرار می‌گیرند، نقایص شناخته شده توسط محققان و کارشناسان امنیتی هستند. دسترسی به سیستم‌های وصله نشده برای مهاجمانی که به دنبال نقص شبکه و ورود به سازمان هستند، آسان است. حتی پس از سال‌ها، وصله کردن (یک تمرین ساده امنیتی)، هنوز به طور موثر اعمال نشده است. در بیشتر سازمان‌ها فرآیندهایی وجود دارد که می‌توان به سرعت وصله‌های منتشر شده از ارائه‌دهندگان را در هنگام بهره‌برداری از آسیب‌پذیری اعمال کرد. وصله کردن موفقیت‌آمیز، باعث کاهش

بهره‌برداری از آسیب‌پذیری، قطعی قابل توجه سیستم، مشکلات در دسترس بودن و ضررهای مالی خواهد شد.

برای کاهش تهدیدات، به سازمان‌ها توصیه می‌شود که دسترسی‌های مدیر سیستم را به‌طور پیش‌فرض حذف کنند. آن‌ها غالباً از آسیب‌پذیری‌های خارجی ناشی از استفاده از برنامه‌های ناامن و سیستم‌عامل‌ها بی اطلاعند. اگر این مسائل هر چه سریع‌تر، به طور مثال در حین یک ارزیابی امنیتی یا توسط یک محقق امنیتی کشف شود (پیش از کشف آن توسط مهاجمان)، آنگاه آسیب‌پذیری می‌تواند وصله شود.

حذف حقوق admin ریسک‌های داخلی ناشی از نصب برنامه‌های مخرب شامل جاسوس‌افزار یا بدافزار که داده‌ها یا پول را سرقت می‌کند، سیستم‌ها را hijack کرده و تجارت را مختل می‌کند، را کاهش می‌دهد. همچنین از ایجاد back-doorهای شخص ثالث جلوگیری کرده و داده‌های حساس غیر قابل دسترس را جهت انتقال، اصلاح یا استخراج، ارائه می‌کند. کاربران می‌توانند با ایجاد تغییراتی، فعالیت کاربران غیرمجاز بیرون از سیستم یا انتشار محتوای آنلاین احراز هویت نشده که می‌تواند باعث آسیب‌هایی به برند شود را مسدود کنند. این یکی از ساده‌ترین و موثرترین روش‌هایی است که هر سازمانی می‌تواند انجام دهد.

امروزه تکنیک‌های مهندسی اجتماعی برای هدف گرفتن کاربران استفاده می‌شوند؛ به طور مثال ارسال یک پیوست مخرب در ایمیل، جهت دسترسی به شبکه‌های سازمانی. به نظر می‌رسد کلیه آسیب‌پذیری‌های موجود در محصولات می‌توانند به عنوان نقطه ورود به سازمان تلقی شده و برای انتشار کد مخرب از آن‌ها استفاده شود.

پیوست یا لینک مخرب می‌تواند برای بهره‌برداری از آسیب‌پذیری در برنامه‌های Internet Explorer، مایکروسافت Edge یا مایکروسافت آفیس استفاده شود. بازگشایی آن توسط کاربر، باعث دسترسی مستقیم مهاجمان به سیستم می‌شود. در صورتی که کاربر دارای دسترسی‌های admin محلی باشد، مهاجم نه تنها به همه فایل‌های سیستم که قابل بارگذاری یا رمزنگاری هستند، دسترسی پیدا می‌کند، بلکه می‌تواند با سرقت اعتبارها به سیستم‌های موجود در شبکه حمله کرده و به سرویس‌ها و دامنه‌های بحرانی دسترسی پیدا کند. همچنین انتشار باج‌افزار در سیستم آسان‌تر می‌شود. اگر اصل حداقل حقوق به خوبی پیاده‌سازی شود و کاربر از امتیازات admin برای امور روزمره استفاده نکند، مهاجم باید جهت افزایش دسترسی‌ها و تأثیر مخرب بر سیستم‌های دیگر، تلاش بیشتری کند.

پیاده سازی اصل حداقل حقوق یکی از مهمترین وظایفی است که سازمان‌ها باید برای محافظت از خود در برابر آسیب‌پذیری‌های ذکر شده انجام دهند. این مسئله، برای وصله کردن نرم‌افزارها و سیستم به منظور حذف کلیه آسیب‌پذیری‌هایی که ممکن است از آن‌ها بهره‌برداری شود، حیاتی است. بهترین محافظت از سیستم‌ها توسط مفاهیمی مانند اصل حداقل حقوق، پیاده‌سازی احرازهویت چند عاملی (MFA) و آموزش/آگاهی حاصل می‌شود.

در بین بدافزارهای رایج، باج‌افزار و فیشینگ بیشترین تهدید را در کاربران اعمال می‌کنند. بسیاری از بدافزارهای سنتی را می‌توان با حذف حقوق amin کاهش داد. حذف حقوق amin تنها در مسائل امنیتی وجود ندارد؛ بلکه باعث می‌شود سیستم‌ها با سرعت بیشتر، بهتر و طولانی‌تر و با نصب‌های مجدد کمتری اجرا شوند. این مسئله مشکل مربوط به باج‌افزارها را حل نمی‌کند، اما می‌تواند باعث کاهش سرعت انتشار آن شود.

یکی دیگر از تهدیدات معمول فیشینگ است؛ این مسئله نمی‌تواند تنها با حفاظت فنی از بین رود. ٪۹۹ از حملات فیشینگ می‌تواند با پیاده‌سازی احرازهویت چند عاملی (MFA) کاهش یابد. در یک درصد باقیمانده، می‌توان با آموزش و افزایش آگاهی با آن مقابله کرد، به همین دلیل باید در کلیه سازمان‌ها حملات فیشینگ شبیه سازی شده همراه با آموزش امنیتی اجباری، انجام شود.

۷ متدولوژی

هر بولتن منتشر شده توسط مایکروسافت شامل یک خلاصه اجرایی همراه با اطلاعات عمومی است. آسیب‌پذیری‌ها با حذف دسترسی‌های admin کاهش یافته و در دسته‌های زیر طبقه‌بندی می‌شوند:

- کاربران/مشتریانی که حساب کاربری آن‌ها با دسترسی کمتر در سیستم پیکربندی شده است، نسبت به کاربرانی که دارای دسترسی‌های admin هستند، کمتر تحت تأثیر قرار می‌گیرند.
- اگر کاربر با دسترسی‌های admin وارد سیستم شود، مهاجم می‌تواند کنترل کامل سیستم تحت تأثیر را به دست گیرد.

۷-۱ نحوه طبقه‌بندی آسیب‌پذیری‌ها

هر آسیب‌پذیری می‌تواند روی یک یا چند محصول تأثیر بگذارد که این مسئله در ماتریسی در صفحه هر آسیب‌پذیری نمایان است. به هر آسیب‌پذیری یک نوع از هفت طبقه بندی زیر اختصاص داده شده است: اجرای کد از راه دور، افشای اطلاعات، انکار سرویس، دور زدن ویژگی امنیتی، کلاه‌برداری، مداخله.

هر نوع از آسیب‌پذیری اغلب مربوط به ترکیبی از نسخه‌های مختلف یک محصول یا محصولات یا بعضی اوقات تمام نسخه‌ها است. همچنین به هر آسیب‌پذیری یک شدت که توسط مایکروسافت رده‌بندی شده است، اختصاص داده می‌شود (بحرانی، مهم، متوسط)، که بسته به نوع هر بخش از نرم‌افزار تحت تأثیر یا ترکیبی از بخش‌های آن متغیر است. سیستم امتیازدهی عمومی آسیب‌پذیری‌ها (CVSS) یک استاندارد منتشر شده است که توسط سازمان‌ها در سراسر جهان استفاده می‌شود و پس از بررسی ویژگی‌های اصلی آسیب‌پذیری، عددی ایجاد می‌شود که نشان دهنده شدت آن آسیب‌پذیری است. شدت عددی می‌تواند جهت

کمک به سازمان‌ها که فرآیندهای مدیریت آسیب‌پذیری خود را ارزیابی و اولویت‌بندی کنند، به صورت کیفی ترجمه شود (مانند پایین، متوسط، بالا و بحرانی).

آسیب‌پذیری‌های خاصی که بر نرم‌افزارهای مختلف اثر می‌گذارند، در سال ۲۰۱۹ چندین بار رخ داده است. در این موارد، کلیه نرم‌افزارها تحت تأثیر یک آسیب‌پذیری خاص قرار گرفته و آسیب‌پذیری فقط یک بار محاسبه می‌شود.

۸ نتیجه‌گیری

هنگامی‌که یک سازمان فرآیندهای بسیار بنیادی را برای امنیت و مدیریت حساب‌های با امتیاز بالا پیاده‌سازی نمی‌کند، خود را در معرض خطرات قابل‌توجهی قرار می‌دهد. حذف امتیازات مدیر سیستم، یک گام مهم و ضروری برای حفظ امنیت اطلاعات و جلوگیری از نشت اطلاعات سازمانی است. سوءاستفاده از دسترسی‌های مدیر سیستم، منجر به زیان بسیار، سرقت اطلاعات و لکه‌دار شدن نشان‌های تجاری می‌شود. سازمان‌ها باید در رابطه با مدیریت دسترسی‌های با امتیاز بالا، بدون ایجاد موانع برای انجام کار، بهترین شیوه‌ها را اجرا کنند. مادامی که این کار را در اسرع وقت انجام داده و یک خط مشی داخلی منسجم برای افزایش یا کاهش دسترسی‌های مدیر سیستم داشته وجود داشته باشد، سازمان‌ها از خطرات بسیاری در امانند.

۹ مراجع

[1] https://www.beyondtrust.com/resources/whitepapers/microsoft-vulnerability-report

[2] https://www.faraasat.com/

[3] https://nextadmin.net/poor-pam-processes-and-policies-leave-the-crown-jewels-susceptible-to-security-breaches/