بهمن

۱۳۹۹

ماهنامه

امنیت فناوری اطلاعات

شبکه گستر

امنیت شما | وظیفه ما

newsroom.shabakeh.net

@SGnewsroom

فهرست مطالب

چکیده مدیریتی

در این شماره از ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر به بررسی مهمترین رخدادها و رویدادهای مرتبط با امنیت فناوری اطلاعات در دی ۱۳۹۹ پرداخته شده است.

در دی ماه، برخی نهادها نسبت به فعالیت گسترده باج‌افزار Egregor بر ضد کسب‌وکارهای خصوصی در کشورهای مختلف هشدار دادند. ایمیل‌های فیشینگ با پیوست‌های مخرب و نفوذ از طریق پودمان‌های غیرامن Remote Desktop Protocol - به اختصار RDP - از جمله روش‌های رخنه اولیه مهاجمان Egregor به شبکه قربانیان گزارش شده است. در این ماهنامه روش کار این باج‌افزار مورد کالبدشکافی و بررسی قرار گرفته است.

در ماهی که گذشت ابعاد گسترده‌تری از حمله زنجیره تأمین سولاروینڈز روشن شد. از جمله می‌توان به شناسایی بدافزارهای جدیدی اشاره کرد که در جریان حمله مذکور مورد استفاده مهاجمان قرار گرفته بوده‌اند. همچنین شرکت مایکروسافت اعلام کرد که مهاجمان پشت‌پرده نفوذ به سولاروینڈز، با هک حساب‌های کاربری این شرکت، موفق به مشاهده کد منبع (Source Code) محصولات آن شده بوده‌اند. مشروح این رویدادها را در این ماهنامه بخوانید.

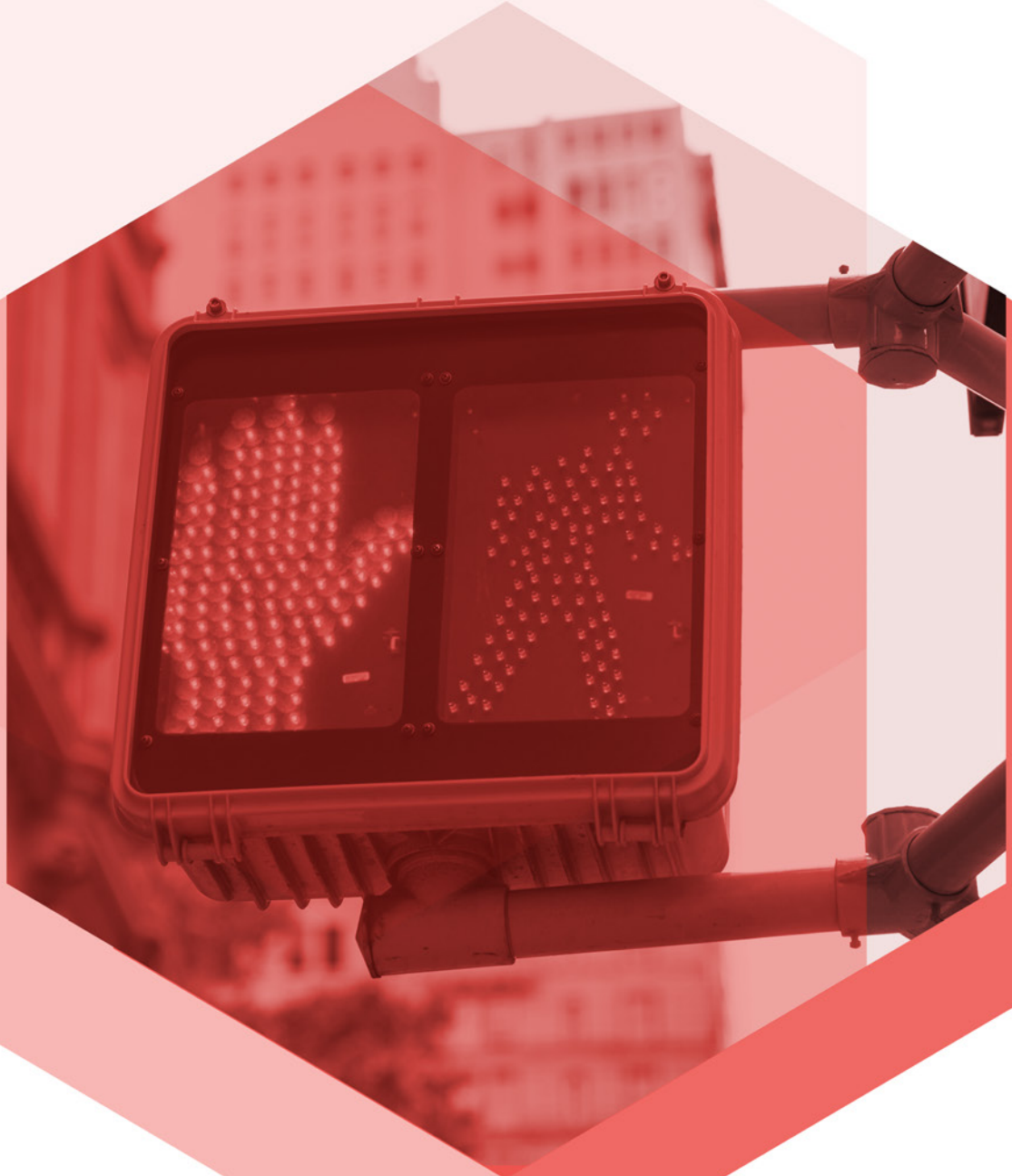
از دیگر رخدادهای مهم در دی ۱۳۹۹ می‌توان به توقف رسمی توزیع نرم‌افزار Flash Player و عرضه اصلاحیه برای آن توسط شرکت ادوبی اشاره کرد. عدم انتشار اصلاحیه‌های امنیتی برای Flash Player به‌معنای آسیب‌پذیری هر چه بیشتر دستگاه‌هایی است که این نرم‌افزار بر روی آنها نصب است. لذا حذف این محصول از روی تمامی دستگاه‌های سازمان به تمامی راهبران توصیه می‌شود. جزییات بیشتر در خصوص پایان حیات این نرم‌افزار در این ماهنامه قابل مطالعه است.

همچنین همان‌طور که در این ماهنامه خواهید خواند شرکت‌های مایکروسافت و مک‌آفی، به همراه ۱۷ شرکت فعال در حوزه فناوری و سازمان غیرانتفاعی، ائتلافی را جهت مقابله مؤثر با باج‌افزارها تشکیل داده‌اند. این ائتلاف که به نیروی ضربت ضدباج‌افزار (Ransomware Task Force - به اختصار RTF) معروف شده بر روی ارزیابی راهکارهای فنی موجود در مقابله مؤثر با حملات باج‌افزاری تمرکز خواهد داشت.

در دهمین ماه ۱۳۹۹، شرکت‌های مایکروسافت، سیسکو، مک‌آفی، بیت‌دیفندر، ادوبی، گوگل، موزیلا، زایکسل، سیتریکس، اس‌آپ و اِنویدیا و بنیاد آپاچی اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند. جزییات این به‌روزرسانی‌ها و گزارش‌های متنوع دیگر را در این ماهنامه بخوانید.

شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب ماهنامه امنیت فناوری اطلاعات شرکت مهندسی شبکه گستر که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

هشدارهای امنیتی



SuperNova؛

دیگر بدافزار توزیع شده توسط سولارویندز

سولارویندز (SolarWinds Inc) با به‌روزرسانی توصیه‌نامه قبلی خود به معرفی بدافزار دیگری با نام SuperNova پرداخته که از طریق یکی از محصولات این شرکت در سطح جهان توزیع شده است.

به گزارش شرکت مهندسی شبکه گستر، در اواسط آذر ماه مشخص شد که در نتیجه اجرای حمله سایبری موفق بر ضد سولارویندز، مهاجمان قادر به تزریق کد آلوده به یکی از فایل‌های نرم‌افزار SolarWinds Orion -با نام SolarWinds.Orion.Core.BusinessLayer.dll - و تبدیل آن به یک درب‌پشتی (Backdoor) که به SUNBURST معروف گردیده شده بودند. فایل مذکور نیز از طریق قابلیت به‌روزرسانی خودکار Orion به شبکه مشتریان سولارویندز راه یافته بود.

بررسی بعدی دو شرکت مایکروسافت (Microsoft Corp) و پالوآلتو نت‌ورکز (Palo Alto Networks Inc) نشان داد که بدافزار دیگری با نام SuperNova نیز با همین تکنیک در کشورهای مختلف منتشر شده است. با این تفاوت که فایل دست‌درازی شده توسط این بدافزار، app_Web_logoimagehandler.ashx.b6031896.dll نام دارد.

SuperNova مهاجمان را قادر می‌کند تا به‌صورت از راه دور کد C# را به دستگاه آلوده ارسال کرده و در ادامه آن را کامپایل و اجرا کنند. هر دو شرکت مایکروسافت و پالوآلتو نت‌ورکز احتمال می‌دهند که گروه پشت‌پرده SuperNova متفاوت از مهاجمان گرداننده SUNBURST باشند.

اکنون سولارویندز با به‌روزرسانی توصیه‌نامه قبلی خود به تهدید SuperNova نیز پرداخته است.

در بخشی از این توصیه‌نامه آمده:

بدافزار SuperNova از دو جزء تشکیل شده است. جزء اول، یک شل وب آلوده و امضا نشده (Unsigned) با نام app_web_logoimagehandler.ashx.b6031896.dll است که به‌طور خاص برای استفاده توسط SolarWinds Orion Plat- form نوشته شده است. جزء دوم نیز بهره‌جوی یک آسیب‌پذیری امنیتی در SolarWinds Orion Platform است که توزیع کد مخرب را ممکن ساخته است.

به تمامی راهبران SolarWinds Orion Platform توصیه شده که در اسرع‌وقت نسبت به ارتقای این محصول به یکی از نسخ زیر اقدام کنند:

- 2019.4 HF 6 (December 14, 2020)
- 2020.2.1 HF 2 (December 15, 2020)
- 2019.2 SUPERNOVA Patch (December 23, 2020)
- 2018.4 SUPERNOVA Patch (December 23, 2020)
- 2018.2 SUPERNOVA Patch (December 23, 2020)

توصیه‌نامه سولارویندز در لینک زیر قابل مطالعه است:

- http://www.solarwinds.com/securityadvisory

توضیح این‌که فایل آلوده app_web_logoimagehandler.ashx.b6031896.dll با نام‌های زیر قابل شناسایی است:

- Bitdefender: Trojan.Supernova.A
- McAfee: Trojan-sunburst
- Sophos: Mal/Generic-S + Mal/Sunburst-B

Flash Player
مرد!

تا ساعاتی دیگر، مصادف با تولد ۲۵ سالگی Flash Player، حیات این نرم‌افزار برای همیشه پایان می‌یابد.

Flash Player فناوری پرطرفداری بود که محتوای تولید شده در بستر آن، خاطرات زیادی را برای چندین نسل از کاربران رقم زده است.

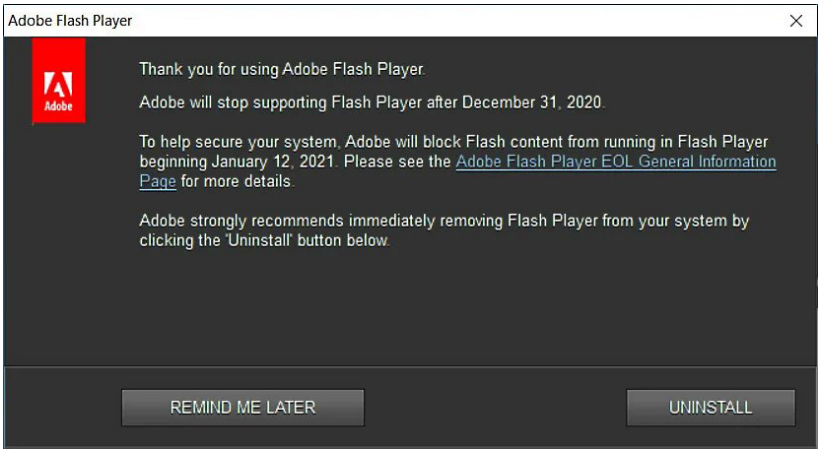
اما امنیت Flash Player همواره یکی از اصلی‌ترین دغدغه‌های محققان امنیت فناوری اطلاعات و منتقدان این نرم‌افزار بوده است.

سالهاست آسیب‌پذیری‌های روز-صفر و حیاتی در این نرم‌افزار مورد سوءاستفاده تبهکاران سایبری، از هکرهای تازه‌کار گرفته تا نفوذگران حرفه‌ای با پشتوانه دولتی قرار می‌گیرد.

اولین بار در مرداد ۱۳۹۶ شرکت ادوبی (Adobe Inc) در بیانیه‌ای مشترک با شرکت‌های اپل (Apple Inc)، فیس‌بوک (Facebook Inc)، گوگل (Google LLC)، مایکروسافت (Microsoft Corp) و موزیلا (Mozilla Corp) از پایان پشتیبانی از Flash Player در انتهای سال ۲۰۲۰ خبر داد. این تصمیم بر پایه کاهش کاربران این نرم‌افزار به دلیل ظهور فناوری‌های امن و کاراتر نظیر HTML۵، WebGL و WebAssembly گرفته شد.

به گزارش شرکت مهندسی شبکه گستر، از فردا ۱۲ دی ماه شرکت ادوبی، رسماً توزیع این نرم‌افزار و عرضه اصلاحیه برای آن را متوقف خواهد کرد.

جهت هشدار به کاربران در خصوص ریسک امنیتی استفاده از این نرم‌افزار، شرکت ادوبی با نمایش پیام‌هایی به کاربران توصیه اکید می‌کند که نسبت به حذف این محصول از روی دستگاه خود اقدام کنند.



با این حال تا زمانی که کاربر بر روی دگمه Uninstall کلیک نکند یا به‌صورت دستی آن را حذف نکند Flash Player همچنان بر روی دستگاه فعال باقی خواهد ماند.

از مدتی پیش نیز، همان‌طور که در اینجا به آن پرداخته شد شرکت مایکروسافت با انتشار یک به‌روزرسانی اختیاری (Optional) به شناسه KB4577586 امکان حذف خودکار نرم‌افزار Flash Player فراهم کرده است.

عدم انتشار اصلاحیه‌های امنیتی برای Flash Player به معنای آسیب‌پذیری هر چه بیشتر دستگاه‌هایی است که این نرم‌افزار بر روی آنها نصب است. لذا حذف این محصول از روی تمامی دستگاه‌های سازمان به تمامی راهبران توصیه می‌شود.

فعالیت گسترده باج‌افزار Egregor

اداره تحقیقات فدرال (FBI) با انتشار یک اطلاعیه امنیتی، نسبت به فعالیت گسترده باج‌افزار Egregor بر ضد کسب‌وکارهای خصوصی در کشورهای مختلف هشدار داده است.

به گفته این نهاد ایالات متحده، از سپتامبر ۲۰۲۰، بیش از ۱۵۰ شرکت، قربانی این باج‌افزار شده‌اند.

به دلیل تعداد بالای مهاجمانی که در توزیع Egregor نقش دارند تاکتیک‌ها، تکنیک‌ها و روال‌های (TTP) استفاده شده در جریان حملات آنها گسترده و متفاوت از یکدیگر است؛ موضوعی که مقابله با این باج‌افزار را دشوار کرده است.

ایمیل‌های فیشینگ با پیوست‌های مخرب و نفوذ از طریق پودمان‌های غیرامن Remote Desktop Protocol - به اختصار RDP - از جمله روش‌های رخنه اولیه مهاجمان به شبکه قربانیان گزارش شده است.

در جریان این حملات، مهاجمان از Cobalt Strike، Qakbot/Qbot، Advanced IP Scanner و AdFind برای ارتقای سطح دسترسی و گسترش دامنه نفوذ خود به سیستم‌های دیگر شبکه بهره می‌گیرند.

همچنین از ابزارهای 7-Zip و Rclone که در پس پروسه svchost توسط مهاجمان استتار شده‌اند در فرایند سرقت اطلاعات پیش از رمزگذاری فایل‌ها سوءاستفاده می‌شود.

در هشدار FBI به بهره‌جویی (Exploit) از آسیب‌پذیری‌های زیر نیز اشاره شده است:

- CVE-2020-0609
- CVE-2020-0610
- CVE-2020-16896
- CVE-2019-1489
- CVE-2019-1225
- CVE-2019-1224
- CVE-2019-1108

Egregor از جمله باج‌افزارهایی است که در قالب خدمات موسوم به "باج‌افزار به‌عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) در اختیار تبهکاران سایبری قرار می‌گیرد.

به گزارش شرکت مهندسی شبکه گستر، در RaaS، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به متقاضی و بخشی دیگر به نویسنده می‌رسد. این سهم در سرویس RaaS باج‌افزار Egregor ۷۰ و ۳۰ درصد است. بدین‌نحو که ۷۰ درصد از مبلغ باج به فرد یا گروهی که کار انتشار Egregor را بر عهده داشته می‌رسد و ۳۰ درصد باقیمانده به برنامه‌نویسان و گردانندگان اصلی Egregor تعلق می‌گیرد.

به‌طور کلی مهاجمان Egregor، اهداف خود را به‌صورت خاص انتخاب کرده و ضمن سرقت فایل‌ها و داده‌ها، در صورت پرداخت نشدن مبلغ اخاذی‌شده اقدام به افشای آنها می‌کنند.

این باج‌افزار پس از آن‌که در آبان ماه گردانندگان Maze رسما اعلام کردند که پروژه باج‌افزاری آنها برای همیشه متوقف شده و سایت آنها دیگر اقدام به افشای داده‌های قربانیان نخواهد کرد بر سر زبان‌ها افتاد.

با رعایت موارد زیر می‌توان سازمان را از گزند این باج‌افزار مخرب ایمن نگاه داشت:

- استفاده از رمزهای عبور پیچیده، هک نشده و غیرتکراری برای حساب‌های کاربری محلی (Local) تحت دامنه (Domain) سیستم عامل و پایگاه‌های داده، به ویژه حساب‌های با سطح دسترسی Administrator/SysAdmin
- محدود کردن سطح دسترسی کاربران
- مدیریت سخت‌گیرانه سطوح دسترسی اعمال شده بر روی پوشه‌های اشتراکی
- پرهیز از قابل دسترس کردن سرویس‌های حساسی نظیر MS-SQL و Domain Controller در بستر اینترنت یا مقاوم‌سازی آنها
- غیرفعال کردن پودمان RDP یا حداقل تغییر درگاه پیش‌فرض آن
- اطمینان از نصب بودن اصلاحیه‌های امنیتی بر روی تمامی دستگاه‌ها
- ارتقای سیستم‌های عامل از رده خارج
- استفاده از ضدویروس قدرتمند و به‌روز با قابلیت نفوذیاب
- استفاده از دیواره آتش و ضدهرزنامه در درگاه شبکه
- فعال‌سازی سیاست‌های مقابله با بدافزارهای "بدون فایل" (Fileless) در محصولات امنیت نقاط پایانی
- رصد اجرای فایل‌های bat، js و vbs؛ برای این منظور می‌توانید از راهکار قدرتمند McAfee Threat Intelligence Exchange بهره بگیرید.

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

اصلاحیه‌های عرضه شده
در دی ۱۳۹۹

در دی ۱۳۹۹، شرکت‌های مایکروسافت، سیسکو، مک‌آفی، بیت‌دیفندر، ادوبی، گوگل، موزیلا، زایکسل، سیتریکس، اس‌آپ و اِنویدیا و بنیاد آپاچی اقدام به عرضه به‌روزرسانی و توصیه‌نامه امنیتی برای برخی محصولات خود کردند.

۲۳ دی، شرکت مایکروسافت (Microsoft Corp) مجموعه‌اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژانویه منتشر کرد. این اصلاحیه‌ها در مجموع، ۸۳ آسیب‌پذیری را در سیستم عامل Windows و طیف وسیعی از سرویس‌ها و نرم‌افزارهای مایکروسافت ترمیم می‌کنند. درجه اهمیت ۱۰ مورد از آسیب‌پذیری‌های ترمیم شده توسط اصلاحیه‌های مذکور "حیاتی" (Critical) و ۷۳ مورد "بااهمیت" (Important) اعلام شده است.

در درجه‌بندی شرکت مایکروسافت، نقاط ضعفی که سوءاستفاده از آنها بدون نیاز به دخالت و اقدام کاربر باشد، "حیاتی" تلقی شده و اصلاحیه‌هایی که این نوع نقاط ضعف را ترمیم می‌کنند، بالاترین درجه اهمیت یا "حیاتی" را دریافت می‌نمایند. نقاط ضعفی که سوءاستفاده موفق از آنها نیازمند فریب کاربر به انجام کاری باشد یا نیازمند دسترسی فیزیکی به دستگاه هدف باشد، توسط اصلاحیه‌هایی با درجه اهمیت "بااهمیت" برطرف و ترمیم می‌گردند.

یکی از آسیب‌پذیری‌های ترمیم شده توسط این مجموعه اصلاحیه‌ها، ضعفی "روز-صفر" (Zero-day) در نرم‌افزار Microsoft Defender است که جزییات آن پیش‌تر افشا شده بود. بهره‌جویی از این آسیب‌پذیری به شناسه CVE-2021-1647 مهاجم را قادر به "اجرای کد به‌صورت از راه دور" (Remote Code Execution) می‌کند. این ضعف امنیتی "روز-صفر" در Microsoft Malware Protection Engine 1.1.17700.4 و نسخ بعد از آن ترمیم شده است.

مایکروسافت همچنین یک آسیب‌پذیری از نوع "ترفیع امتیازی" (Elevation of Privilege) با شناسه CVE-2021-1648 را در بخش splwow۶۴ سیستم عامل Windows ترمیم کرده است. Google Project Zero در سپتامبر ۲۰۲۰ جزییات این آسیب‌پذیری را، البته با شناسه CVE-2020-0986 منتشر کرده بود.

مایکروسافت در ۱۸ دی ماه نیز با انتشار نسخه ۸۷.۰.۶۶۴.۷۵ نرم‌افزار Edge، ۱۳ آسیب‌پذیری امنیتی را در نسخه موسوم به Chromium-based این مرورگر ترمیم کرده بود. جزییات بیشتر در لینک زیر قابل دریافت است:

- https://msrc.microsoft.com/update-guide/vulnerability/ADV200002

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه اصلاحیه‌های ماه ژانویه مایکروسافت در لینک زیر قابل دریافت و مطالعه است:

- https://newsroom.shabakeh.net/21974

لازم به ذکر است که هفته گذشته 0patch اقدام به عرضه یک Micropatch برای ترمیم ضعفی از نوع ترفیع امتیازی در ابزار PsExec کرد. PsExec یکی از برنامه‌های ارائه شده در مجموعه Sysinternals است که راهبران را قادر به اجرای کد به‌صورت از راه دور می‌کند. اگر چه PsExec جزیی از Windows نیست اما توسط بسیاری از راهبران و نرم‌افزارهای سازمانی برای اجرای از راه دور برنامه‌ها، انجام به‌روزرسانی یا فراخوانی سایر فرامین مدیریتی مورد استفاده قرار می‌گیرد. لذا با توجه به فراگیری استفاده از آن به ویژه در بسترهای سازمانی، استفاده از این Micropatch که در لینک زیر در دسترس قرار گرفته توصیه شده است.

- https://blog.0patch.com/2021/01/local-privilege-escalation-0day-in.html

توضیح این که مایکروسافت اصلاحیه رسمی برای آسیب‌پذیری مذکور عرضه نکرده است.

شرکت سیسکو (Cisco Systems Inc) در دی ماه در چندین نوبت اقدام به عرضه اصلاحیه‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها در مجموع، ۳۱ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۸ مورد از آنها "بالا" (High) گزارش شده است. آسیب‌پذیری به حملاتی همچون "اجرای کد به‌صورت از راه دور"، "تزریق کد از طریق سایت" (Cross-Site Scripting) و "از کاراندازی سرویس" (Denial of Service) از جمله اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

- https://tools.cisco.com/security/center/publicationListing.x

در دی ۱۳۹۹ شرکت امنیتی مک‌آفی (McAfee Corp) اقدام به عرضه نسخ جدید برای برخی از محصولات امنیت نقاط پایانی و امنیت اطلاعات خود کرد. از جمله موارد لحاظ شده در به‌روزرسانی‌های جدید می‌توان به پشتیبانی از بسترهای جدید، افزایش قابلیت‌ها و ترمیم آسیب‌پذیری‌های امنیتی و برطرف شدن باگ‌های عملکردی اشاره کرد. جزییات بیشتر در لینک‌های زیر قابل دریافت است:

- McAfee Agent 5.7.1 (https://docs.mcafee.com/bundle/agent-5.7.x-release-notes-epolicy-orchestrator)
- Endpoint Security for Linux 10.7.3 (https://docs.mcafee.com/bundle/endpoint-security-10.7.3-threat-prevention-release-notes-linux)

در دهمین ماه از سال ۱۳۹۹ شرکت بیت‌دیفندر اقدام به انتشار نسخ ۶.۶.۲۳.۳۲۹ و ۴.۱۵.۱۲۴.۲۰۰۱۲۴ به‌ترتیب برای محصولات Endpoint Security Tools for Windows و Endpoint Security for Mac و افزودن قابلیت‌های جدید در آنها کرد. جزییات بیشتر را در لینک‌های زیر بخوانید:

- https://www.bitdefender.com/support/bitdefender-endpoint-security-tools-version-6-6-23-329-release-notes-(windows)-2647.html
- https://www.bitdefender.com/support/endpoint-security-for-mac-version-4-15-124-200124-release-notes-2648.html

ادوبی (Adobe Inc) نیز در دی ماه، چندین آسیب‌پذیری را در محصولات زیر ترمیم و اصلاح کرد:

- Photoshop (https://helpx.adobe.com/security/products/photoshop/apsb21-01.html)
- Illustrator (https://helpx.adobe.com/security/products/illustrator/apsb21-02.html)
- Animate (https://helpx.adobe.com/security/products/animate/apsb21-03.html)
- Campaign Classic (https://helpx.adobe.com/security/products/campaign/apsb21-04.html)
- InCopy (https://helpx.adobe.com/security/products/incopy/apsb21-05.html)
- Captivate (https://helpx.adobe.com/security/products/captivate/apsb21-06.html)
- Bridge (https://helpx.adobe.com/security/products/bridge/apsb21-07.html)

لازم به ذکر است که ۱۲ دی ماه شرکت ادوبی، رسماً توزیع نرم‌افزار Flash Player و عرضه اصلاحیه برای آن را متوقف کرد. عدم انتشار اصلاحیه‌های امنیتی برای Flash Player به‌معنای آسیب‌پذیری هر چه بیشتر دستگاه‌هایی است که این نرم‌افزار بر روی آنها نصب است. لذا حذف این محصول از روی تمامی دستگاه‌های سازمان به تمامی راهبران توصیه می‌شود. جزییات بیشتر در خصوص پایان حیات این نرم‌افزار در لینک زیر قابل مطالعه است:

- https://newsroom.shabakeh.net/21951

در ۱۷ دی شرکت گوگل (Google LLC) با عرضه نسخه ۸۷.۰.۴۲۸۰.۱۴۱ اقدام به ترمیم ۱۶ آسیب‌پذیری‌های امنیتی مرورگر Chrome کرد. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

- https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop.html

در ماهی که گذشت شرکت موزیلا (Mozilla Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. درجه حساسیت همه این آسیب‌پذیری‌های ترمیم شده، "حیاتی" گزارش شده است. توضیحات بیشتر در لینک‌های زیر قابل مطالعه است:

- https://www.mozilla.org/en-US/security/advisories/mfsa2021-01/
- https://www.mozilla.org/en-US/security/advisories/mfsa2021-02/

به تازگی نیز شرکت زایکسل (Zyxel Communications Corp)، یک آسیب‌پذیری حیاتی را در ثابت‌افزار (Firmware) دستگاه‌های خود ترمیم کرده است. ضعف امنیتی مذکور که به آن شناسه CVE-2020-29583 تخصیص داده شده از وجود یک حساب کاربری مخفی و مستندنشده در کد ثابت‌افزار ناشی می‌شود. بهره‌جویی از CVE-2020-29583 مهاجم را قادر به در اختیار گرفتن کنترل دستگاه با سطح دسترسی admin می‌کند. جزییات بیشتر در مورد آسیب‌پذیری مذکور و روش اصلاح آن در مطلبی که مرکز مدیریت راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر آن را تهیه کرده قابل مطالعه است:

- https://afta.gov.ir/portal/home/?news/235046/237266/242532/

بر طبق اعلام سیتریکس (Citrix Systems, Inc)، مهاجمان، محصولات Citrix ADC و Citrix Gateway را هدف حمله DDoS قرار داده‌اند. در نتیجه اجرای این حمله، توان عملیاتی Citrix ADC DTLS کاهش یافته و به‌طور بالقوه پهنای باند خروجی اشغال می‌شود.

پیامد این حمله بر روی ارتباطات با پهنای باند محدود، شدیدتر است. Datagram Transport Layer Security - به اختصار DTLS - پودمانی است که هدف آن امن کردن ارتباطات برنامه‌ها و سرویس‌های حساس به تأخیر (Delay-sensitive) در بستر Datagram Transport است. به‌تازگی این شرکت قابلیتی با عنوان را HelloVerifyRequest در نسخ جدید ثابت‌افزارهای خود لحاظ کرده که موجب بی‌اثر شدن این حملات می‌شود. جزییات کامل این حملات و راهکار سیتریکس در لینک زیر قابل دریافت و مطالعه است:

- https://afta.gov.ir/portal/home/?news/235046/237266/242560/

اس‌آپ (SAP SE) دیگر شرکتی بود که در دی ماه ۹۹ با انتشار به‌روزرسانی امنیتی، آسیب‌پذیری‌هایی را در چندین محصول خود برطرف کرد. بهره‌جویی از بعضی از این آسیب‌پذیری‌های ترمیم شده مهاجم را قادر به در اختیار گرفتن کنترل سیستم می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

- https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=564760476

در دی، بنیاد نرم‌افزاری آپاچی (Apache Software Foundation)، ضعفی به شناسه CVE-2021-24122 را در Apache Tomcat منتشر کرد که سوءاستفاده از آن مهاجم را قادر به دستیابی به اطلاعات بالقوه حساس می‌کند. اطلاعات بیشتر در لینک زیر در دسترس است:

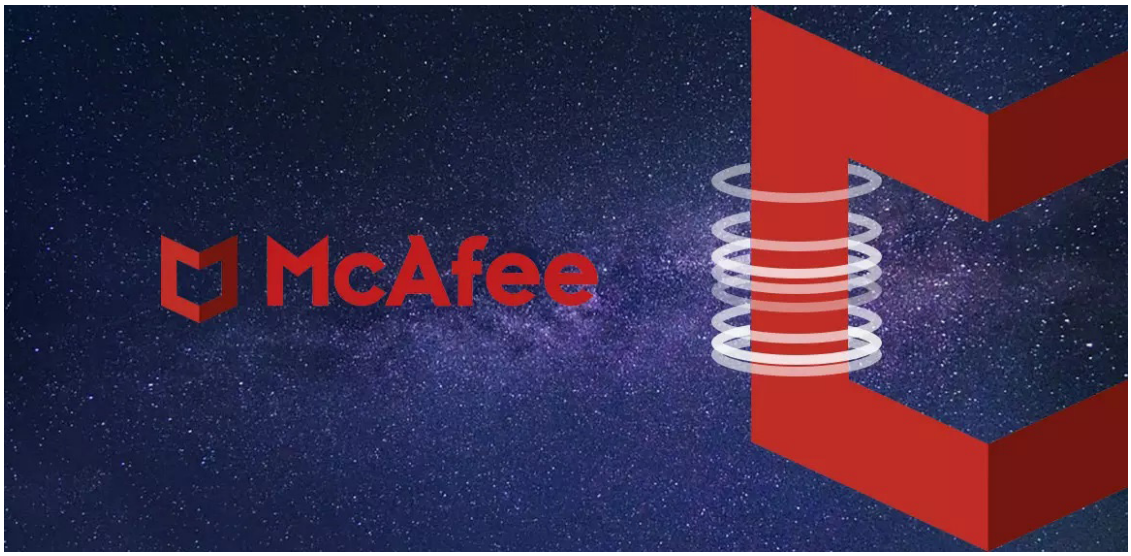
- https://us-cert.cisa.gov/ncas/current-activity/2021/01/15/apache-releases-security-advisory-tomcat

۲۲ دی، اِنویدیا (Nvidia Corp) با انتشار به‌روزرسانی‌های امنیتی، چندین آسیب‌پذیری را در محصولات GPU و Virtual GPU - به اختصار vGPU - ساخت این شرکت ترمیم و اصلاح کرده است. راه‌اندازهای GPU (در بسترهای Windows و Linux) از شش مورد و نرم‌افزارهای vGPU از ده مورد از این آسیب‌پذیری‌های ترمیم‌شده تأثیر می‌پذیرند. جزییات بیشتر را در گزارش مرکز مدیریت راهبردی افتای ریاست جمهوری که با مشارکت شرکت مهندسی شبکه گستر تهیه شده قابل دسترس است:

- https://afta.gov.ir/portal/home/?news/235046/237266/242577/

رویدادها و وقایع امنیتی

چند نکته در خصوص امضای
نسخ جدید محصولات مک‌آفی



به دلایل امنیتی فایل‌های نسخ جدید محصولات شرکت امنیتی مک‌آفی (McAfee Corp) توسط گواهینامه‌های جدید امضا شده‌اند. اعتبارسنجی فایل‌های دودویی امضا شده (Signed Binaries) مستلزم وجود گواهینامه‌های موسوم به Root به‌روزشده بر روی سیستم عامل است. شرکت مایکروسافت (Microsoft Corp) به‌صورت خودکار این گواهینامه‌ها را بر روی سیستم عامل Windows توزیع می‌کند. اما در صورت عدم اتصال دستگاه به اینترنت یا غیرفعال بودن RootAutoUpdate ممکن است فرایند نصب یا ارتقای نسخ جدید مک‌آفی با مشکل روبرو شود.

در این مواقع توصیه می‌شود که با دنبال کردن یکی از مراحل زیر این گواهینامه‌های Root به سیستم عامل معرفی شوند:

- فایل bat.txt از اینجا دریافت شده و نام آن به USERFirst_and_VeriSign_and_Comodo_and_GlobalSign_and_USERTrust.bat تغییر داده شود. در ادامه فایل بر روی سیستم اجرا شود.
- و یا فایل reg.txt از اینجا دریافت شده و نام آن به USERFirst_and_VeriSign_and_Comodo_and_GlobalSign_and_USERTrust.reg تغییر داده شود. در ادامه فایل در محضرخانه (Registry) سیستم عامل وارد (Import) شود.

با اجرای هر یک از مراحل مذکور گواهینامه‌های زیر به سیستم عامل معرفی می‌شوند:

- AAA Certificate Services (2028)
- AddTrust External CA Root (2020)
- AddTrust External CA Root (2023)
- COMODO RSA Code Signing CA (2028)
- GlobalSign (2029)
- GlobalSign (2028)
- GlobalSign CodeSigning CA - SHA256 - G3 (2024)
- GlobalSign CodeSigning CA - G3 (2024)
- GlobalSign Root CA (2021)
- GlobalSign Root CA (2028)
- McAfee Code Signing CA 2 (2024)
- McAfee OV SSL CA 2 (2024)
- Microsoft Code Verification Root (2025)

- USERTrust RSA Certification Authority (2020)
- USERTrust RSA Certification Authority (2028)
- USERTrust RSA Certification Authority (2038)
- UTN-USERFirst-Object (2019)
- Verisign Class 3 Code Signing 2010 CA (2020)
- Verisign Class 3 Public Primary Certification Authority - G5 (2036)
- Verisign Universal Root Certification Authority (2037)

همچنین علیرغم پایان پشتیبانی شرکت مایکروسافت از Windows 7 و Windows Server 2008/2008 R2 از ۲۵ دیماه ۱۳۹۸ و توقف عرضه رایگان اصلاحیه‌های امنیتی برای آن، بر اساس اعلام قبلی مک‌آفی پشتیبانی محصولات این شرکت از سیستم‌های عامل مذکور حداقل تا ۱۰ دی ۱۴۰۰ ادامه خواهد یافت. جزییات بیشتر در این خصوص در لینک زیر قابل مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=KB91432

لازم به ذکر است که نسخ جدید محصولات مک‌آفی از جمله McAfee Endpoint Security و McAfee VirusScan Enterprise 8.8 Patch 15+ از گواهینامه‌های دیجیتال SHA-2 استفاده می‌کنند (جزییات بیشتر در لینک زیر).

https://kc.mcafee.com/corporate/index?page=content&id=KB92382

شرکت مایکروسافت به‌منظور پشتیبانی از گواهینامه‌های مبتنی بر SHA-2، به‌روزرسانی KB4474419 را برای سیستم‌های عامل Windows 7 و Windows Server 2008/2008 R2 منتشر کرده است. به‌روزرسانی مذکور به‌صورت خودکار بر روی این سیستم‌های عامل نصب و اجرا می‌شود. اما در صورت عدم اتصال دستگاه به اینترنت یا WSUS (با پیکربندی صحیح) نیاز است که KB4474419 به‌صورت دستی بر روی سیستم‌های عامل مذکور توزیع و نصب شود. در غیر اینصورت ممکن است که فرایند نصب یا ارتقای نسخ جدید مک‌آفی بر روی این سیستم‌های عامل با موفقیت صورت نگیرد.

به‌روزرسانی KB4474419 از مسیر زیر قابل دریافت است:

https://www.catalog.update.microsoft.com/search.aspx?q=kb4474419

جزییات بیشتر در مورد KB4474419 نیز در لینک زیر قابل مطالعه است:

https://support.microsoft.com/en-us/help/4474419/sha-2-code-signing-support-update

اتحاد مایکروسافت و مک‌آفی
در مقابله با باج‌افزارها

شرکت‌های مایکروسافت (Microsoft Corp) و مک‌آفی (McAfee Corp)، به همراه ۱۷ شرکت فعال در حوزه فناوری و سازمان غیرانتفاعی، ائتلافی را جهت مقابله مؤثر با باج‌افزارها تشکیل داده‌اند.

این ائتلاف که به نیروی ضربت ضدباج‌افزار (Ransomware Task Force - به اختصار RTF) معروف شده بر روی ارزیابی راهکارهای فنی موجود در مقابله مؤثر با حملات باج‌افزاری تمرکز خواهد داشت.

فهرست ۱۹ شرکت و سازمان تشکیل‌دهنده این ائتلاف به‌شرح زیر است:

- Microsoft
- McAfee
- Aspen Digital
- Citrix
- The Cyber Threat Alliance
- Cybereason
- The CyberPeace Institute
- The Cybersecurity Coalition
- The Global Cyber Alliance
- The Institute for Security and Technology
- Rapid۷
- Resilience
- SecurityScorecard
- Shadowserver Foundation
- Stratigos Security
- Team Cymru
- Third Way
- UT Austin Stauss Center
- Venable LLP

به گزارش شرکت مهندسی شبکه گستر، RTF قصد دارد تا با تدوین یک نقشه راه، اشکالات و نقاط ضعف راهکارهای موجود را برطرف کند.

در حالی است که فروشندگان ضدویروس از توانایی محصولاتشان در شناسایی باج‌افزارها و بی‌اثر کردن حملات باج‌افزاری تمجید می‌کنند در یک سال اخیر گروه‌هایی از مهاجمان با اجرای حملاتی هدفمند و پیچیده موفق به اخاذی ده‌ها میلیون دلار از قربانیان خود - علیرغم استفاده از محصولات امنیتی پیشرفته و به‌روز - شده‌اند. منافع بالای مالی سبب گردیده که شمار مهاجمان حرفه‌ای که به جمع گردانندگان حملات باج افزاری ملحق می‌شوند هر روز بیشتر از قبل شود.

چارچوبی استاندارد و جامع برای مقابله مؤثر با تهدیدات باج‌افزاری باشد، RTF انتظار می‌رود که خروجی ائتلاف.

دسترسی هکرهای سولارویندز
به کد نرم‌افزارهای مایکروسافت

شرکت مایکروسافت (Microsoft Corp) اعلام کرده که مهاجمان پشت‌پرده نفوذ به سولارویندز، با هک حساب‌های کاربری این شرکت، موفق به مشاهده کد منبع (Source Code) محصولات آن شده‌اند.

به گزارش شرکت مهندسی شبکه گستر، در آذر ماه، مهاجمان پس از هک شرکت سولارویندز و آلوده‌سازی یکی از فایل‌های نرم‌افزار Orion، آن را به یک درب‌پشتی (Backdoor) تبدیل کردند و در عمل موجب شدند که شبکه مشتریان این نرم‌افزار در هر نقطه از جهان به تسخیر آنها در بیاید.

مدتی بعد از افشای این حمله زنجیره تأمین (Supply Chain)، شرکت‌های مطرح متعدد از جمله مایکروسافت تایید کردند که به سبب استفاده از SolarWinds Orion، برخی سیستم‌های آنها برای مدتها در کنترل مهاجمان بوده است.

بر طبق اعلام مایکروسافت مهاجمان این حملات، موفق به هک چندین حساب کاربری شده بودند. مهاجمان از یکی از حساب‌های مذکور برای مشاهده کد منبع نرم‌افزارهای مایکروسافت استفاده کرده‌اند. در عین حال سطح دسترسی این حساب کاربری محدود به مشاهده کدها بوده و امکان اعمال هر گونه تغییر در آنها را نداشته است. مایکروسافت تأکید کرده که سندی دال بر اینکه مهاجمان موفق به دستیابی به داده‌های مشتریان این شرکت شده باشند نیافته است.

در بیانیه مایکروسافت اشاره شده در رویکرد امنیتی این شرکت فرض بر آن است که مهاجمان همیشه به کد منبع محصولات دسترسی دارند. لذا علیرغم اثبات مشاهده شدن کد توسط این مهاجمان، مایکروسافت آن را یک ریسک امنیتی تلقی نمی‌کند.

مشروح بیانیه مایکروسافت در لینک زیر قابل مطالعه است:

https://msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/

افتای ریاست جمهوری با همکاری شبکه گستر

شبکه گستر

شرکت مهندسی شبکه گستر

در دی ماه مرکز مدیریت راهبردی افتای ریاست جمهوری با همکاری شرکت مهندسی شبکه گستر اقدام به تهیه گزارش‌های زیر کرد.

ترمیم چند آسیب‌پذیری با درجه حساسیت بالا در محصولات QNAP

کیونپ با انتشار به‌روزرسانی‌های امنیتی، چندین آسیب‌پذیری با درجه حساسیت بالا را در تجهیزات ذخیره‌ساز متصل به شبکه (NAS) این شرکت ترمیم کرده است. ادامه مطلب را در اینجا بخوانید.

اجرای حملات DDoS بر ضد محصولات شبکه‌ای Citrix

مهاجمان در حال اجرای حملات DDoS بر ضد محصولات Citrix ADC هستند. ادامه مطلب را در اینجا بخوانید.

افشای دو آسیب‌پذیری حیاتی در استک Treck TCP/IP

جزییات چهار آسیب‌پذیری در استک موسوم به Treck TCP/IP به‌صورت عمومی در دسترس قرار گرفته است. مرکز CISA ایالات متحده نیز با انتشار توصیه‌نامه‌ای نسبت به تأثیر آسیب‌پذیری‌های مذکور بر روی سامانه‌های کنترل صنعتی (ICS) هشدار داده است. ادامه مطلب را در اینجا بخوانید.

استخراج ارز رمز بر روی Linux و Windows، توسط بدافزاری چندبستری

محققان از شناسایی بدافزاری جدید با عملکرد "کرم" خبر داده‌اند که از اوایل دسامبر ۲۰۲۰ اقدام به نصب ابزار XMRig و استخراج ارز رمز مونرو بر روی دستگاه‌های با سیستم عامل Windows و Linux می‌کند. ادامه مطلب را در اینجا بخوانید.

کشف یک حساب کاربری مخفی در تجهیزات Zyxel

شرکت تایوانی Zyxel، یک آسیب‌پذیری حیاتی را در ثابت‌افزار دستگاه‌های خود ترمیم کرده است. ضعف امنیتی مذکور که به آن شناسه CVE-۲۰۲۰-۲۹۵۸۳ تخصیص داده شده از وجود یک حساب کاربری مخفی در کد ثابت‌افزار ناشی می‌شود. ادامه مطلب را در اینجا بخوانید.

Sunburst؛ نشانه‌های آلودگی و راهکارهای مقابله

در اواسط آذر ماه فاش شد که مهاجمان با اجرای یک حمله سایبری موفق بر ضد شرکت سولارویندز، اقدام به تزریق کد آلوده به یکی از فایل‌های نرم‌افزار SolarWinds Orion و تبدیل آن به یک "درب‌پشتی" با نام SUNBURST شده بودند. ادامه مطلب را در اینجا بخوانید.

راهکار جدید Citrix در مقابله با حملات مبتنی DTLS

همان‌طور که پیش‌تر اشاره شده بود بر طبق اعلام شرکت سیتریکس، مهاجمان، محصولات Citrix ADC و Citrix Gateway را هدف حمله DDoS قرار داده‌اند. اکنون این شرکت قابلیتی با عنوان HelloVerifyRequest را در نسخ جدید ثابت‌افزارهای خود لحاظ کرده که موجب بی‌اثر شدن این حملات می‌شود. ادامه مطلب را در اینجا بخوانید.

Babuk Locker؛ اولین باج افزار سازمانی ۲۰۲۱

باج‌افزار Babuk Locker تهدید سازمانی جدیدی است که از ابتدای سال ۲۰۲۱ شروع به فعالیت کرده و تا کنون موفق به آلوده‌سازی چند شرکت در نقاط مختلف جهان و سرقت اطلاعات از آنها شده است. مبالغ اخاذی شده از قربانیان بین ۶۰ تا ۸۵ هزار دلار است که در قالب بیت‌کوین دریافت می‌شود. ادامه مطلب را در اینجا بخوانید.

ترمیم آسیب‌پذیری‌های حیاتی توسط NVIDIA

انویدیا با انتشار به‌روزرسانی‌های امنیتی، چندین آسیب‌پذیری را در محصولات GPU و vGPU ساخت این شرکت ترمیم و اصلاح کرده است. سوءاستفاده از این آسیب‌پذیری‌ها منجر به از کار افتادن خدمات‌دهی دستگاه، ترفیع سطح دسترسی، تغییر یافتن داده‌ها و نشت اطلاعات می‌شود. ادامه مطلب را در اینجا بخوانید.

افشای چند آسیب‌پذیری روز-صفر در محصولات Rockwell Automation

بر اساس توصیه‌نامه‌ای که از سوی Rockwell Automation منتشر شده محققان در مجموع چهار آسیب‌پذیری از نوع DoS را در دو محصول این شرکت کشف کرده‌اند. شرکت Rockwell Automation یکی از معروف ترین سازندگان تجهیزات الکتریکی است.

شرکت Rockwell Automation یکی از معروف ترین سازندگان تجهیزات الکتریکی است. ادامه مطلب را در اینجا بخوانید.

Sunspot؛ سومین بدافزار کشف شده در جریان هک SolarWinds

شرکت امنیتی CrowdStrike اعلام کرده که سومین بدافزار بکار رفته توسط گردانندگان هک SolarWinds را کشف کرده است.

از این بدافزار جدید با عنوان Sunspot یاد شده و اکنون نام آن در کنار دو بدافزار شناسایی شده قبلی، یعنی، Sunburst و Teardrop قرار می‌گیرد. ادامه مطلب را در اینجا بخوانید.

آخـرین اخبـار امنیـت فنـاوری اطلاعات

@SGnewsroom

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۴۲۰۵۲ - ۰۲۱
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net