بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و هفتم

آذرماه ۱۳۹۹

بزرگ‌ترین حمله سایبری قرن!

solarwinds

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:
مرکز تخصصـــی آپـا دانشگـاه رازی

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

سردبیران:
سیده مرضیه حسینی
صبا آزرمی

با همکاری:
سیده‌آرزو حسنی
پویا شکری

آدرس:
کرمانشـــاه، باغ ابریشـــم، دانشـــگاه رازی، دانشکده برق و کامپیوتر، طبقه همکف، مرکز تخصصی آپا

۰۸۳۳۴۳۴۳۲۵۱
apa@razi.ac.ir
@APARazi
cert.razi.ac.ir

اخبار امنیتی

هک آژانس‌های ایالات متحده و FireEye با استفاده از Backdoor در نرم‌افزار SolarWinds

مهاجمان تحت حمایت دولت روسیه، سازمان خزانه‌داری آمریکا، اداره ملی مخابرات و اطلاعات، وزارت بازرگانی و دیگر سازمان‌های دولتی را هدف قرار داده‌اند تا ترافیک ایمیل داخلی را به عنوان بخشی از کمپین گسترده جاسوسی سایبری خود، زیر نظر داشته باشند.

هنوز به طور کامل انگیزه مهاجمان و دامنه اطلاعات به خطر افتاده مشخص نیست، اما سازمان امنیتی FireEye مدعی شد، مهاجمان که گمان می‌رود به نمایندگی از یک دولت خارجی فعالیت می‌کنند، سرور نرم افزار SolarWinds را مورد تهاجم قرار داده‌اند و سپس یک به‌روزرسانی lock بدافزار، برای نرم‌افزار Orion به منظور آلوده کردن شبکه‌های شرکت‌های متعدد آمریکایی و شبکه‌های دولتی منتشر کرده‌اند.

همچنین منابعی که با واشنگتن پست مصاحبه می‌کردند، نفوذ و تهاجم را به APT29 مرتبط دانستند، نام رمزی که صنعت امنیت سایبری برای توصیف هکرهای مرتبط با سرویس اطلاعات خارجی روسیه به کار می‌گیرد. هرچند که FireEye هنوز APT29 را به عنوان مهاجم به طور رسمی تأیید نکرده است و به گروه مهاجم یک نام رمز مستعار به نام UNC2452 داده است، اما منابع متعددی در جامعه امنیت سایبری، بر اساس شواهد موجود، تهاجم را از سوی APT29 می‌دانند. همان گروهی که چند روز پیش سرقت ابزارهای تست نفوذ Red Team را ترتیب داده بود.

مهاجمان از طریق به‌روزرسانی ORION بدافزار SUNBURST خود را در شبکه قرار داده‌اند. براندون ولز، سرپرست آژانس امنیت سایبری و امنیت زیرساخت‌های آمریکا که یک دستورالعمل اضطراری منتشر کرده است، از سازمان‌های غیرنظامی فدرال خواست شبکه‌های خود را برای مواجهه با فعالیت‌های مشکوک مورد بررسی قرار داده و قطع ارتباط با محصولات SolarWinds Orion را بلافاصله در دستور کار خود قرار دهند.

محصولات شبکه‌ای و امنیتی SolarWind توسط بیش از ۳۰۰,۰۰۰ مشتری در سراسر جهان از جمله ۵۰۰ شرکت، سازمان‌های دولتی و موسسات آموزشی مورد استفاده قرار می‌گیرند. همچنین در شرکت‌های بزرگ مخابراتی آمریکا، هر

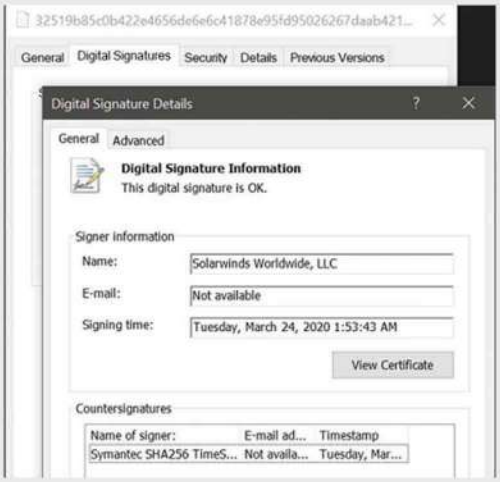
[1] Forum

هر پنج شعبه ارتش آمریکا و دیگر سازمان‌های برجسته دولتی مانند پنتاگون، وزارت امور خارجه، ناسا، آژانس امنیت ملی، خدمات پستی، NOAA، وزارت دادگستری، و دفتر رئیس جمهوری ایالات متحده، مورد استفاده است.

کمپین تهاجم برای توزیع و انتشار SUNBURST Backdoor

این تهاجم با نام SUPPLY CHAIN، با استفاده از تروجان در SolarWinds Orion، منجر به به‌روزرسانی نرم‌افزار به منظور توزیع یک درب پشتی به نام SUNBURST شد .

FireEye در یک مصاحبه مدعی شد: این کمپین ممکن است از اوایل بهار ۲۰۲۰ آغاز شده باشد و در حال حاضر نیز در حال فعالیت است.



این نسخه تهاجمی از SolarWinds Orion، علاوه بر masquerading ، برای برقراری ارتباط از طریق پروتکل HTTP با سرورهای از راه دور، ترافیک شبکه خود را به عنوان برنامه بهبود دهنده Orion (OIP) معرفی می‌کند.

برنامه بهبود Orion یا همان OIP، به طور کلی برای ارزیابی عملکرد و استفاده آماری از داده‌های مربوط به کاربران SolarWinds به منظور بهبود محصول مورد استفاده قرار می‌گیرد.

مایکروسافت در رابطه با این موضوع گفت: یک کلاس نرم‌افزاری مخرب در میان بسیاری از کلاس‌های مشروع دیگر گنجانده شده و سپس با گواهی مشروع، تأیید هویت صورت گرفته است و حاصل آن، ایجاد یک در پشتی بود به مرور در سازمان‌های مورد هدف توزیع شد.

مشاوره امنیتی SolarWinds

در یک مشاوره امنیتی منتشر شده توسط SolarWinds، این شرکت مدعی شده که این حملات نسخه‌های ۲۰۱۹.۴ تا ۱.۲.۲۰۲۰ از نرم‌افزار SolarWinds Orion را هدف قرار می‌دهد که بین ماه‌های مارس و ژوئن ۲۰۲۰ منتشر شده‌اند، به‌علاوه این شرکت به کاربران خود توصیه کرده بلافاصله نسخه ارتقاء یافته ۱.۰.۲۰۲۰ HF1 را نصب کنند.

این شرکت در حال حاضر در حال بررسی این حمله با همکاری FireEye و اداره تحقیقات فدرال آمریکا است. همچنین انتظار میرود در ۱۵ دسامبر یک هات فیکس به نام HF1 ۱.۲.۲۰۲۰ منتشر کند که جایگزین مؤلفه‌ی تسخیر شده می‌شود و تعدادی قابلیت امنیتی اضافه نیز ارائه می‌کند.

FireEye نام این بدافزار را SUNBURST گذاشت و همچنین برای تشخیص آن، در GitHub یک گزارش فنی منتشر کرد. مایکروسافت نیز نام بدافزار را Solorigate گذاشت و قوانین تشخیص را به آنتی ویروس خود اضافه کرد.

ابزارهای نفوذی که از Red Team به سرقت رفته، ترکیبی از ابزارهای در دسترس عموم (۴۳٪)، نسخه‌های اصلاح شده ابزارهای در دسترس عموم (۱۷٪) و ابزارهایی که منحصراً توسعه یافته‌اند (۴۰٪) می‌باشد. علاوه براین، سرقت شامل payloadهای اکسپلویت و سوءاستفاده از آسیب‌پذیری‌های بحرانی نیز می‌باشد که برخی از آن‌ها عبارتند از:

Pulse Secure SSL VPN (CVE-2019-11510)

Microsoft Active Directory (CVE-2020-1472)

Zoho ManageEngine Desktop Central (CVE-2020-10189)

Windows Remote Desktop Services (CVE-2019-0708)

به نظر می‌رسد این حمله، یک حمله SUPPLY CHAIN در مقیاس جهانی است، زیرا FireEye مدعی شده که این فعالیت در چندین نهاد در سراسر جهان تشخیص داده شده است، در دولت‌ها، سازمان‌های فناوری، مخابرات، و شرکت‌هایی در آمریکای شمالی، اروپا، آسیا و خاورمیانه.

منبع خبر :

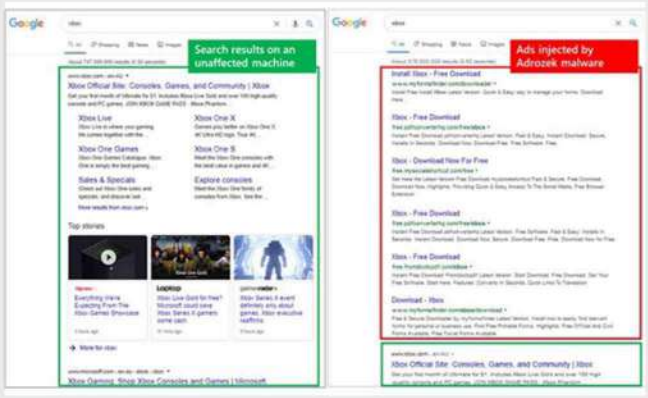
Scan Link

بدافزار Adrozek در چهار مرورگر وب

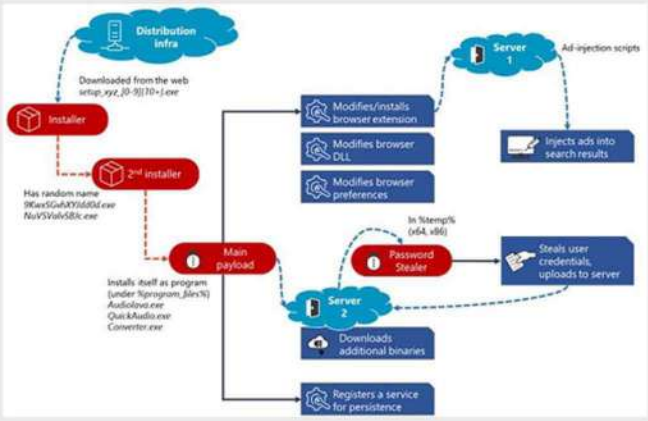
شرکت مایکروسافت از وجود نقص امنیتی در چند مرورگر وب خبر داد. این نقص که توسط تیم تحقیقاتی Microsoft 365 Defender Research، "Adrozek" نامیده شده است، به طور پنهانی تبلیغات آلوده به بدافزار را به نتایج جستجو تزریق می‌کند تا از این طریق، مهاجم پشت پرده، کسب درآمد کند. این بدافزار ۱۵۹ دامنه منحصر بفرد دارد که هر یک از آن‌ها به طور متوسط میزبان ۱۷,۳۰۰ URL منحصربفرد هستند. این نقص امنیتی بر روی مرورگرهای Yandex Browser، Google Chrome، Microsoft Edge و Mozilla Firefox ویندوز تأثیر می‌گذارد و عملکرد آن به گونه‌ای است که تبلیغات اضافی و غیرمجاز را در بالای تبلیغات قانونی موجود در صفحات نتایج موتورهای جستجو درج خواهد کرد که این عمل باعث می‌شود کاربران ناخواسته بر روی این تبلیغات کلیک کنند.

به گفته کارشناسان شرکت مایکروسافت، این بدافزار از ماه مه ۲۰۲۰ فعالیت خود را آغاز

و در اوج خود در ماه آگوست، هر روز بیش از ۳۰،۰۰۰ دستگاه را تحت تأثیر قرار داده است.



باتوجه به آن که بدافزار Adrozek بر چندین مرورگر وب تأثیر می‌گذارد، نشان دهنده آن است که دارای مکانیزم پیچیدای می‌باشد، علاوه بر این، بدافزار مذکور به دلیل ماندگاری بالا، اطلاعات وب‌سایت را از بین برده و دستگاه‌های آسیب‌دیده را در معرض خطرات دیگری نیز قرار خواهد داد. Adrozek پس از نصب بر روی سیستم هدف، اقدام به ایجاد تغییر در تنظیمات مرورگر و کنترل‌های امنیتی می‌کند تا افزونه‌های مخرب را بدون رضایت کاربر، نصب کند. اگرچه مرورگرهای مدرن، جهت جلوگیری از ایجاد اختلال و دستکاری‌های احتمالی، از کنترل‌های خاصی استفاده می‌کنند؛ اما این بدافزار به طرز هوشمندانه‌ای این ویژگی را غیرفعال می‌کند و به مهاجم اجازه خواهد داد تا کنترل‌های امنیتی را دور بزند. همچنین بدافزار مذکور برای واکشی اسکریپت‌های اضافه، از سرورهای راه دور، جهت تزریق تبلیغات جعلی استفاده می‌کند که این امر با هدف کسب درآمد صورت می‌پذیرد.

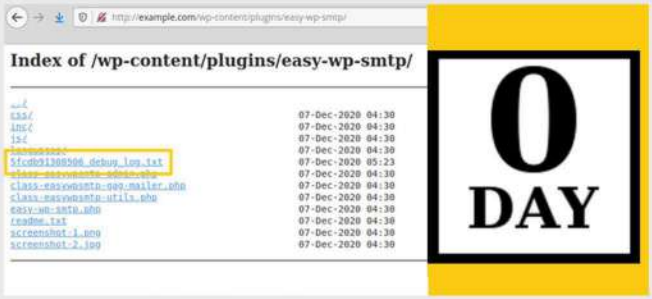


عملکرد بدافزار Adrozek، در مرورگر Mozilla Firefox، یک گام فراتر رفته، اطلاعات را به سرقت می‌برد و داده‌ها را به سرورهای کنترل شده توسط مهاجم منتقل خواهد کرد. لذا توصیه می‌شود کاربرانی که از مرورگرهای Google Chrome، Yandex Browser و Mozilla Firefox استفاده می‌کنند، در اسرع وقت مرورگرهای خود را بروزرسانی کنند تا از گزند این بدافزار در امان باشند.

منبع خبر :

Scan Link

آسیب‌پذیری روزصفرم در افزونه Easy WP SMTP وردپرس



Easy WP SMTP یک افزونه وردپرس با بیش از ۵۰۰،۰۰۰ نصب، به کاربران امکان می‌دهد تا کلیه ایمیل‌های خروجی را از طریق یک سرور SMTP، پیکربندی و ارسال کنند. مهم‌ترین مزیت این افزونه این است که ایمیل‌ها در پوشه junk یا spam گیرنده قرار نمی‌گیرند.

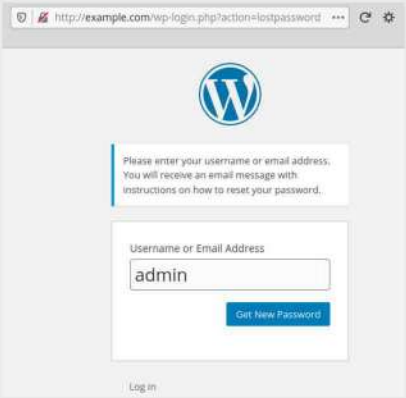
تیم مدیریت‌کننده این افزونه، آسیب‌پذیری روز صفر را در نسخه‌های تحت تأثیر آن یعنی ۱.۴.۲ و نسخه‌های پایین‌تر از آن برطرف کرده است (آخرین نسخه ۱.۴.۴). به موجب این آسیب‌پذیری یک کاربر احراز هویت نشده می‌تواند رمز ورود کاربر admin را بازنشانی کند که این امر باعث می‌شود هکر بتواند کنترل کامل وب‌سایت را به‌دست گیرد.

این نقص امنیتی در یک فایل دیباگ وجود دارد که به دلیل وجود خطا در چگونگی حفاظت پلاگین از یک پوشه ایجاد می‌شود. افزونه Easy WP SMTP دارای یک debug log اختیاری است که در آن کلیه ایمیل‌های ارسال شده توسط وبلاگ را می‌نویسد و در پوشه نصب افزونه، به آدرس " /wp-content/plugins/easy-wp-smtp/ " قرار دارد. این لاگ، یک فایل متنی با یک نام تصادفی مانند 5fcdb91308506_debug_log.txt می‌باشد.

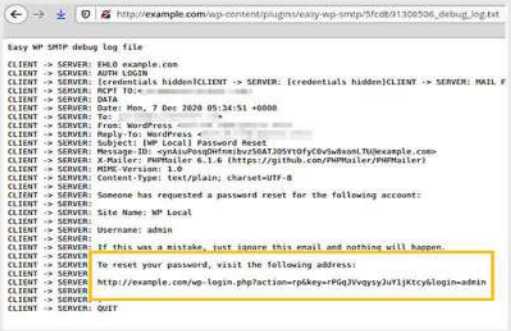
شایان ذکر است که پوشه پلاگین، هیچ فایل index.htmlای ندارد و از این رو هکرها می‌توانند در سرورهایی که directory listing فعال دارند، لاگ را مانند تصویر زیر پیدا کرده و مشاهده کنند.

در مرحله بعدی، اسکن نام‌کاربری جهت یافتن "admin login"، انجام خواهد شد.

همچنین هکرها می‌توانند از طریق دستور (/?author=1) نیز این کار را انجام دهند. آن‌ها مانند تصویر زیر به صفحه ورود به سیستم دسترسی پیدا کرده و درخواست بازنشانی رمز ورود ادمین را اعمال می‌کنند.



سپس مجدداً به debug log افزونه Easy WP SMTP دسترسی می‌گیرند تا لینک جدیدی که توسط WordPress ارسال خواهد شد را کپی کنند.



هکر پس از دریافت لینک، رمزعبور ادمین را بازنشانی خواهد کرد.

در نهایت پس از ورود به داشبورد ادمین، افزونه‌های مخرب نصب شده‌اند؛ لذا با توجه به اهمیت این موضوع، به کاربران توصیه می‌شود هر چه سریع‌تر نسبت به نصب بروزرسانی این افزونه اقدام نمایند.

منبع خبر :

Scan Link

هشدار در خصوص انتشار واسط‌های پیکربندی تجهیزات شبکه و امنیتی سازمان‌ها

رصد فضای سایبری کشور نشان از آن دارد که تعداد قابل توجهی از صفحات پیکربندی فایروال‌های سازمان‌ها، صفحات پیکربندی مسیریاب‌ها، صفحات مانیتورینگ شبکه وغیره از طریق شبکه‌ی اینترنت قابل دسترسی است. این در حالی‌ست که متأسفانه در تعداد قابل توجهی از آن‌ها از کلمه‌ی عبور پیش‌فرض هم استفاده شده است. در این ماه متأسفانه مرکز ماهر بیش از ۲۰۰ مورد هشدار به سازمان‌ها و شرکت‌ها و تولیدکنندگان محصولات امنیتی داخلی ارسال کرده است.

لازم است که دسترسی به این سرویس‌ها از طریق اینترنت محدود شده و اگر بنابر ضرورت‌های کرونایی نیاز به دسترسی راه دور دارد، حتما از طریق vpn انجام اقدام شود. از آن مهم‌تر، نسبت به تغییر کلمات عبور پیش‌فرض حتماً اقدام شود.

منبع خبر :

Scan Link

اخبار کوتاه

شناسایی عامل کلاهبرداری رایانه‌ای

فردی که در سایت‌های خرید و فروش اقدام به کلاهبرداری رایانه‌ای از شهروندان می‌نمود، شناسایی و دستگیری شد.

متهم با بارگذاری آگهی در سایت‌های فروش اینترنتی اقدام به فریب کاربران شبکه‌های اجتماعی می‌کند و با روش‌های متقلبانه خود پس از جلب اعتماد قربانیان به بهانه ارسال جنس مبالغ زیادی از آن‌ها دریافت نموده و سپس با بهانه‌هایی مانند ورشکستگی از ارسال کالا خودداری می‌کرده است. با اقدامات تخصصی و فنی انجام شده توسط کارشناسان سایبری و استخراج مستندات لازم و ادله دیجیتال و هماهنگی با مقام قضایی، بلافاصله حساب مربوطه مسدود شد و متهم مورد شناسایی قرار گرفت. به هموطنان توصیه می‌شود قبل از تحویل کالا از واریز وجه خودداری کنند و در صورت مشاهده هرگونه موارد مجرمانه در فضای مجازی موضوع را به مراتب زیر ربط اطلاع دهند.

آسیب‌پذیری

آسیب‌پذیری در ابزار OpenSSL

این آسیب‌پذیری با شناسه CVE-2020-1971 و شدت بالا، یک نقص بازخوانی[۱] اشاره‌گر Null در ابزار OpenSSL است که موجب خطای قطعه‌بندی[۲] یا نقص دسترسی به حافظه می‌شود. این اتفاق زمانی رخ می‌دهد که برنامه‌ای برای خواندن یا نوشتن در حافظه با اشاره‌گر Null تلاش می‌کند. این آسیب‌پذیری در تابع GENERAL_NAME_cmp از ابزار OpenSSL وجود دارد و زمانی می‌تواند مشکل ایجاد کند که هر دو پارامتر آن از یک نوع باشند (یعنی EDIPARTYNAME).

X.509 GeneralName یک نوع[۳] عمومی برای نمایش انواع مختلف نام‌ها است. یکی از این انواع نام، EDIPartyName می‌باشد. OpenSSL از تابع GENERAL_NAME_cmp برای مقایسه‌ی نمونه‌های مختلف GENERAL_NAME استفاده می‌کند و برابری یا نابرابری آن‌ها را می‌سنجد. این تابع زمانی که هر دو GENERAL_NAME حاوی EDIPARTYNAME باشند درست عمل نمی‌کند، در نتیجه، خطای NULL pointer dereference رخ داده و می‌تواند منجر به حمله‌ی منع سرویس شود. در واقع، OpenSSL از این تابع به دو منظور استفاده می‌کند، اول، مقایسه‌ی نام‌های CRL distribution point[۴] بین CRL موجود و CRL distribution point تعبیه شده در گواهی X509 و دوم، هنگام تأیید مطابقت امضاء کننده‌ی توکنِ پاسخِ timestamp با نام اعتبار timestamp (که از طریق توابع TS_RESP_verify_response و TS_RESP_verify_token نشان داده می‌شود). بنابراین، اگر مهاجم بتواند هر دو پارامترِ تحت مقایسه را کنترل کند آن‌گاه می‌تواند برنامه‌ای را که از OpenSSL استفاده می‌کند از کار بیندازد. به عنوان مثال، اگر مهاجم بتواند کلاینت یا سرور را فریب دهد که گواهی مخرب را با یک CRL مخرب بررسی کند، در این صورت این اتفاق رخ خواهد داد. این بدان معناست که نسخه‌های آسیب‌پذیر OpenSSL نمی‌توانند رمزگذاری صحیح EDIPARTYNAME را تجزیه[۵] کنند، بنابراین، می‌توان EDIPARTYNAME مخرب ساخت که توسط تجزیه‌کننده‌ی OpenSSL پذیرفته شود و حمله آغاز گردد.

---

۱ Dereference
۲ Segmentation
۳ Type
۴ Certificate Revocation List
۵ Parse

نکته قابل توجه این است که برخی از برنامه‌ها به صورت خودکار CRLها را بر اساس URL تعبیه شده در گواهی دانلود می‌کنند. این عمل، پیش از تأیید امضاهای گواهی و تأیید CRL انجام می‌شود. دلیل این امر آن است که s_server و s_client و ابزارهای تأیید در OpenSSL، گزینه‌ی " -crl_download " را پشتیبانی می‌کنند و همین موضوع موجب دانلود خودکار CRL می‌شود که این CRL می‌تواند مخرب باشد.

روش شناسایی این آسیب‌پذیری بدین صورت است که، برنامه‌هایی که با OpenSSL دارای تابع GENERAL_NAME_cmp کامپایل می‌شوند آسیب‌پذیر هستند. اگر تابع GENERAL_NAME_cmp مورد استفاده قرار نگیرد برنامه آسیب‌پذیر نیست.

نسخه‌های تحت تأثیر آسیب‌پذیری

این آسیب‌پذیری، OpenSSL نسخه‌های ۱.۱.۱ و ۱.۰.۲ (تمام نسخه‌های ۱.۱.۱ و ۱.۰.۲) را تحت تأثیر قرار می‌دهد. سایر نسخه‌های OpenSSL نیز پشتیبانی نمی‌شوند و بنابراین مورد بررسی قرار نگرفته‌اند.

روش‌های کاهش / رفع

آسیب‌پذیری مذکور در نسخه‌های ۱.۱.۱i و ۱.۰.۲x برطرف شده است. البته لازم به ذکر است که نسخه‌ی ۱.۰.۲ توسط OpenSSL پشتیبانی نمی‌شود و به‌روزرسانی‌های عمومی را دریافت نمی‌کند، بنابراین تنها کاربران Premium این نسخه، می‌توانند نسخه‌ی به‌روزرسانی شده‌ی ۱.۰.۲x دریافت نمایند.

منبع خبر :

Scan Link

آسیب‌پذیری روزصفرم در نرم‌افزار HPE Systems Insight

این آسیب‌پذیری با شناسه CVE-2020-7200 و شدت بحرانی (۹.۸ از ۱۰)، یک نقص بالقوه در نرم‌افزار HPE Systems Insight Manager (SIM) برای پلتفرم‌های ویندوز و لینوکس است، که برای مهاجم امکان اجرای کد از راه دور را فراهم می‌کند. SIM یک نرم‌افزار مدیریت و پشتیبانی از راه دور برای سرورها، دستگاه‌های ذخیره‌سازی و محصولات شبکه‌ی شرکت HPE می‌باشد.

این نقص ناشی از عدم اعتبارسنجی مناسب داده‌های تأمین شده توسط کاربر است که می‌تواند منجر به Deserialization[1] داده‌های نامعتبر شود، این امر امکان اجرای کد در سرورهای دارای نرم‌افزار آسیب‌پذیر را برای مهاجم فراهم می‌کند. بدین معنا که مهاجم فاقد امتیاز دسترسی می‌تواند با یک حمله‌ی نه چندان دشوار که نیاز به تعامل با کاربر ندارد، از این آسیب‌پذیری بهره‌برداری نماید.

سیستم‌هایی که از نرم‌افزار HPE Systems Insight Manager (SIM) ۷.۶.x استفاده می‌کنند، آسیب‌پذیر هستند.

نسخه‌های تحت تأثیر آسیب‌پذیری

این آسیب‌پذیری، نسخه‌ی ۷.۶.x از نرم‌افزار HPE Systems Insight Manager (SIM) را تحت تأثیر قرار می‌دهد.

روش‌های کاهش / رفع

آسیب‌پذیری مذکور در نسخه‌ی بعدی نرم‌افزار به طور کامل برطرف خواهد شد، اما برای نسخه‌های فعلی در سیستم‌عامل‌های ویندوزی[2] مراحل راهکار کاهش خطر به شرح زیر می‌باشد:

۱. سرویس HPE SIM متوقف گردد.

۲. فایل simsearch.war با دستور زیر از مسیر نصب نرم‌افزار حذف شود:

```
del /Q /F C:\Program Files\HP\Systems Insight Manager\jboss\-
server\hpsim\deploy\simsearch.war
```

۳. سرویس HPE SIM ریستارت شود.

۴. پس از در دسترس قرار گرفتن صفحه‌ی https://SIM_IP:50000، دستور زیر در command prompt اجرا گردد:

```
mxtool -r -f tools\multi-cms-search.xml 1>nul 2>nul
```

منبع خبر :

Scan Link

آسیب‌پذیری در آنتی‌ویروس BitdefenderManager

این آسیب‌پذیری با شناسه CVE-2020-15733 و شدت متوسط (۶.۵ از ۱۰)، در واقع نقص Origin Validation Error در آنتی‌ویروس Bitdefender Plus است، که در آن نرم‌افزار نمی‌تواند اعتبار منبع داده یا ارتباط را به درستی تأیید کند. این آسیب‌پذیری در مؤلفه‌ی SafePay وجود دارد و به منابع وب اجازه می‌دهد که خود را در نوار URL معرفی نکنند.

[1] فرآیند تبدیل جریان بایت به داده

[2] اگرچه HPE SIM هر دو سیستم‌عامل ویندوز و لینوکس را پشتیبانی می‌کند، اما در حال حاضر، تنها راهکار کاهش خطر در سیستم‌های ویندوزی توسط شرکت HPE ارائه شده است.

دستکاری با ورودی ناشناخته منجر به ارتقاء سطح دسترسی در آنتی‌ویروس می‌گردد و به مهاجم امکان دسترسی به هر گونه عملکرد قابل استفاده برای منبع را می‌دهد.

نسخه‌های تحت تأثیر آسیب‌پذیری

این آسیب‌پذیری، نسخه‌های قبل از نسخه‌ی ۲۵.۰.۷.۲۹ از آنتی‌ویروس Bitdefender Antivirus Plus را تحت تأثیر قرار می‌دهد.

روش‌های کاهش/رفع

آسیب‌پذیری مذکور در نسخه‌ی ۲۵.۰.۷.۲۹ برطرف شده است.

منبع خبر :

Scan Link

اخبار کوتاه

تصاویر شخصی در فضای مجازی، طعمه‌ای برای مجرمان سایبری

فردی که با سوءاستفاده از تصاویر دختران جوان اقدام به ایجاد مزاحمت برای آنان می‌کرد، توسط پلیس فتا شناسایی شد. در روند رسیدگی به پرونده مشخص شد که از تصاویر موجود در پروفایل و صفحات شبکه‌های اجتماعی شاکیان سوء استفاده شده و در شبکه‌های اجتماعی تلگرام و اینستاگرام موجب آبروریزی و هتک حیثیت کاربران شده است. کاربران فضای مجازی توجه داشته باشند که عدم توجه به حریم خصوصی در این فضا و به خصوص شبکه‌های اجتماعی می‌تواند زمینه‌ساز مشکلات و گرفتاری برای آن‌ها باشد.

مسدود شدن ۳۷۹ کارت بانکی در رابطه با سایت‌های قمار با گردش حساب میلیاردی

کارشناسان پلیس فتا پس انجام تحقیقات تکمیلی توانستند ۳۷۹ عدد کارت بانکی با گردش حساب تقریبی ۲۳ میلیارد و ۴۵۰ میلیون تومان را مسدود کنند. کاربران باید هشیار باشند و بدانند که فعالیت در سایت‌های شرط‌بندی و حتی با برنده شدن اعضاء، هیچ تضمینی برای دریافت جایزه و یا پول وجود ندارد و در بیشتر موارد، مدیران سایت اقدام به مسدودسازی حساب کاربری افراد می‌نمایند که پس از آن کاربران هیچ‌گونه دسترسی به حساب کاربری خود ندارد و تمام سرمایه خود را به راحتی از دست خواهند داد؛ لذا از همه افراد به خصوص قشر نوجوان و جوان انتظار می‌رود از فعالیت در چنین سایت‌هایی خودداری و به تبلیغات فریبنده آن‌ها توجهی نکنند.

دانش‌آموزان ساده‌ترین شکار مجرمان سایبری

مجرمان سایبری در تماس با دانش‌آموزان از طریق تلفن یا شبکه‌های اجتماعی با وعده‌های واهی مانند و بیان جملاتی مبنی بر انتخاب دانش آموز به عنوان منتخب منطقه، شهرستان، شهر و حتی استان، آن‌ها را فریب می‌دهند. آن‌ها با دروغ جذابی همچون وعده‌ی ارسال بسته آموزشی رایگان به ارزش چند میلیون تومان که شامل کتب و سی‌دی‌های کمک آموزشی است و با پرداخت هزینه پست آن یا ارائه تخفیف ۵۰ درصدی که در صورت واریز هزینه پست یا واریز ۵۰ درصد قیمت این بسته آموزشی، تا یک هفته از طریق پست به دست آن‌ها می‌رسد، دانش‌آموزان را فریب می‌دهد. توصیه می‌شود فرزندان بدون هماهنگی و اطلاع والدین به هیچ عنوان اقدام به خرید آنلاین نکنند و در پی تماس با آن‌ها برای فروش یا ارسال هرگونه کالا یا خدماتی حتما به والدین خود اطلاع بدهند تا در دام مجرمان سایبری گرفتار نشوند.

سوءاستفاده شرکت‌های نظارتی از تبلیغات موبایل برای تخمین موقعیت مکانی دقیق کاربر

یک شرکت اسرائیلی با سوءاستفاده از داده‌های تبلیغات موبایلی، موقعیت مکانی کاربران را با خطای یک متر به دست می‌آورد. شرکت Bsightful با ساخت DSPهای جعلی اطلاعات کاربران را به راحتی از توسعه‌دهندگان اپ جمع‌آوری می‌کند. این پلتفرم‌ها برای رد گم کردن مشابه پلتفرم‌های حقیقی عمل کرده و تبلیغات را نمایش می‌دهند، اما هدف اصلی آن‌ها جمع‌آوری اطلاعات کاربران و فروش آن‌ها به دولت‌ها، پلیس و سازمان‌های دیگر گزارش شده است. دقت داشته باشید که احتمال ردیابی موقعیت مکانی کاربرانی که با جدی گرفتن توصیه‌های حفاظت از حریم خصوصی با دقت مجوزهای دسترسی اپ‌ها را بررسی کرده و از برنامه‌های مسدودسازی تبلیغات استفاده می‌کنند، بسیار سخت‌تر خواهد شد.

اتصال وای‌فای خودکار را غیرفعال کنید!

از آنجا که قابلیت در سال‌های اخیر به یکی از WPS (Wi-Fi Protected Setup) نقاط ضعف مودم‌ها تبدیل شده و امکان دسترسی غیرمجاز به آن با ابزارهایی ساده را به افراد خلافکار می‌دهد؛ لذا به کاربران توصیه می‌شود این قابلیت را غیرفعال کنید. این قابلیت که به معنی راه‌اندازی محافظت‌شده وای‌فای است، امکان اتصال دستگاه‌ها از طریق Pin هشت رقمی به وای‌فای را می‌دهد. برای جلوگیری از هک وای‌فای در زمان خروج از منزل و محل کار خود wifi گوشی یا دستگاه خود را غیرفعال کنید، با انجام این کار علاوه بر حفظ باتری گوشی می‌توانید از حریم خصوصی خود محافظت کنید. تأکید می‌شود هنگام اتصال بهwifiهای عمومی محتاط باشید، همه شبکه‌های وای‌فای عمومی برای حریم شخصی و امنیت کاربران خود احترام قائل نیستند و حتی ممکن است برخی از شبکه‌های عمومی توسط هکرهایی تنظیم شوند که می‌خواهند قربانیان را فریب دهند تا رمزها و حساب‌های بانکی خود را دزدی کنند.

مقالات آموزشی

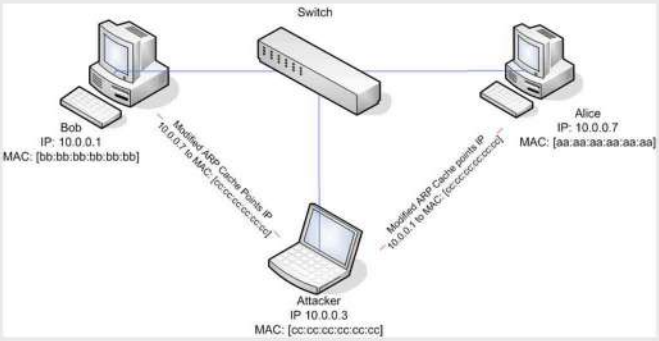
ARP Spoofing و راهکارهای امن‌سازی آن

ARP Spoofing تکنیکی است که در آن مهاجم پیام‌های جعلی ARP را به شبکه محلی ارسال می‌کند. در اصل، هدف قرار دادن آدرس مک (MAC Address) مهاجم به همراه آدرس IP میزبانی دیگر (همچون درگاه پیش فرض) است، که باعث می‌شود به جای اینکه هر ترافیکی که قرار است به آن میزبان ارسال شود، به مهاجم ارسال گردد.

جعل ARP به مهاجم این امکان را می‌دهد که فریم‌های داده را بر روی شبکه محلی از هم جدا کند، ترافیک را تغییر دهد، یا کل ترافیک را متوقف نماید. اغلب این حمله به عنوان ورودی دیگر حملات استفاده می‌شود. از جمله حملاتی نظیر MITM، DOS و Snifing را می‌توان نام برد.

قابل ذکر است این حمله فقط در شبکه‌هایی امکان‌پذیر است که از ARP استفاده می‌کنند و به سگمنت‌های محلی محدود شده‌اند.

طریقه ایجاد جدول مک به این صورت است که سوئیچ با دریافت بسته از هر درگاه و آدرس فرستنده، بسته را به درگاه دریافت کننده اختصاص می‌دهد.



نکته مهم: برای اینکه درخواست ARP پیوسته در شبکه ارسال نشود و ترافیک بیهوده ایجاد نگردد. هر کلاینت یک بار این درخواست را ارسال کرده و سپس جواب‌های ارسالی را به صورت یک جدول در ARP Cache نگه‌داری می‌کند. این جدول شامل Mapping بین IP و MAC می‌باشد. اما هر بار که این درخواست توسط کلاینت دریافت شود جدول ARP Cache خود را update می‌کند و نفوذگر با استفاده از update این جدول حمله خود را انجام می‌دهد.

راهکارهای مقابله با حمله ARP Spoofing چیست؟

۱. تعریف دستی آدرس‌های مک (MAC Address)

برای جلوگیری از این حمله در شبکه‌های بسیار کوچک بهتر است که MAC Address مربوط به سیستم‌ها را به صورت دستی به ARP Cache کلاینت‌ها اضافه کنید. برای این

می‌توانید از دستور arp -s و با وارد کردن IP و MAC در cmd کلاینت‌ها طبق دستور ذیل این کار را انجام دهید با این روش نفوذگر نمی‌تواند با بازنویسی کردن ARP Cache گذرگاه اقدام به ARP Spoofing کند.

```
arp -s 192.168.10.1 a1-1f-fa-c4-e6-e6
```

۲. فعال کردن DIA (Dynamic ARP Inspection)

برای جلوگیری از حمله ARP Spoofing در شبکه‌های بزرگ باید از قابلیت DIA که توسط شرکت سیسکو برای رفع این مشکل عرضه شده استفاده کنید. این ویژگی بسیار شبیه مکانیزم DHCP Spoofing می‌باشد که در بسیاری از موارد این دو باید با هم همراه شوند یعنی هر دو قابلیت باید استفاده شود. قابل ذکر است که باید قبل از فعال کردن DAI ویژگی DHCP Spoofing راه اندازی شود. یعنی با فعال کردن DHCP Spoofing یک جدول ایجاد خواهد شد که سیستم ARP Inspction از آن استفاده می‌کند.

این توانمندی از پورت‌های Trusted و UnTrusted استفاده می‌کند که در این شرایط فقط پورت‌های سوئیچ که در وضعیت Trusted باشند قادر به دریافت پاسخ ARP خواهند بود و در صورتی که یک درخواست ARP از طریق پورت UnTrusted دریافت شود اطلاعات آن با جدول DHCP Binding مقایسه خواهد شد در صورتی که با این جدول مطابقت نداشته باشد حذف خواهد شد و پورت غیرفعال می‌گردد.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
```

تعیین پورت Trusted: به صورت پیش فرض پس از فعال کردن DIA کلیه پورت‌ها در وضعیت UnTrusted قرار خواهند گرفت و شما باید پورت یا پورت‌هایی را که می‌خواهید را در وضعیت Trusted قرار بگیرند را تعیین کنید. برای این منظور از دستور زیر استفاده نمایید، دستور ذیل باعث می‌شود پورت در وضعیت Trusted قرار بگیرد.

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# ip arp inspection trust
```

۳. استفاده از ACL (Access List)

راهکار دیگری که توسط شرکت سیسکو ارائه شده استفاده از Access List می‌باشد. این راهکار برای Static ARP است. زیرا بسیاری از IP ها با DHCP اختصاص داده نمی‌شوند. جهت به کارگیری این روش بایستی همانند پیکربندی ذیل عمل کنید.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# arp access list static arp
Switch(config-acl)# permit ip host 192.168.11.10 mac
host 05a5.e0a1.efa2
Switch(config-acl)#exit
Switch(config)# ip arp inspection filter static arp vlan 1
Switch(config)# interface fastethernet 0/2
Switch(config-if)# ip arp inspection trust
```

اخبار کوتاه

شناسایی عامل ترویج‌دهنده انجام رفتار منافی عفت در اینستاگرام

کارشناسان با رصد فضای‌سایبری، صفحه‌ای را در شبکه اجتماعی اینستاگرام شناسایی کردند که با الگوبرداری از پیج‌های مبتذل غربی اقدام به انتشار محتوای غیراخلاقی برای مخاطبین کرده و آنان را به انجام اعمال منافی عفت تشویق می‌کرد. با انجام اقدامات فنی و تخصصی کارآگاهان سایبری و هماهنگی مراجع قضایی، متهم مورد شناسایی قرار گرفت و دستگیر شد و در نهایت ادله جرم به آزمایشگاه بررسی ادله سایبری منتقل شد. به خانواده‌ها توصیه می‌شود که بدانند نظارت بر فعالیت سایبری فرزندان مثل فضای حقیقی امری طبیعی و الزامی است و خانواده‌ها باید با دوستی با فرزند خود و اختصاص وقت و توجه بیشتر، از آنان در این فضا مراقبت کنند.

هکرها بیش از ۸۵ هزار دیتابیس MySQL را به فروش گذاشتند

بیش از ۸۵ هزار دیتابیس MySQL با قیمت تقریبی ۵۵۰ دلار به ازای هر دیتابیس در یکی از پرتال‌های دارک وب به فروش گذاشته شد.

هکرها از ابتدای سال ۲۰۲۰ تاکنون با نفوذ به سیستم‌ها دیتابیس‌های MySQL را پاک کرده و از قربانی برای دریافت نسخه کپی باج خواهی کرده‌اند. هکرها با راه‌اندازی پرتال از قربانیان درخواست کرده‌اند تا نام کاربری خود را که از طرف هکرها به آن‌ها ارسال شده در سیستم وارد کرده و به صفحه خرید اطلاعات بروند. اگر قربانی در مهلت ۹ روزه پول را پرداخت نکند، اطلاعات او در بخش دیگری از پرتال به حراج گذاشته می‌شود.

هزینه بازیابی دیتابیس باید با بیت کوین پرداخت شود و فارغ از محتویات حدوداً ۵۰۰ دلار به ازای هر دیتابیس است. این موضوع نشان می‌دهد که حملات نفوذ به دیتابیس‌ها و باج خواهی صفحات اینترنتی در حال خودکار شدن هستند و هکرها دیگر داده‌های پدیتابیس‌های هک شده را برای برآورد قیمت تحلیل نمی‌کنند.

حملات باج‌خواهی از طریق سرقت دیتابیس‌ها در سال ۲۰۲۰ روندی صعودی داشت و بسیاری از کاربران در سایت‌هایی همچون ردیت، فروم MySQL، فروم‌های پشتیبانی فنی، سایت Medium و بلاگ‌های شخصی از سرقت دیتابیس‌ها و باج خواهی هکرها شکایت کرده‌اند.

Critical Patch Update Released

مرکز تخصصی آپا دانشگاه رازی