بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره بیست و یکم

خرداد ماه ۱۳۹۹

هشدار به کاربران واتس‌اپ!

در این شماره می‌خوانید :

فهرست

صاحب امتیاز:

مرکز تخصصـــی آپـا دانشگـاه رازی

صفحه آرایی: **سید احسان حسینی**

سردبیران:

سیده مرضیه حسینی

صبا آزرمی

با همکاری

سیده آرزو حسنی

آدرس:

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

۰۸۳۳۴۳۴۳۲۵۱ apa@razi.ac.ir

@APARazi cert.razi.ac.ir

اخبار امنیتی

هدف حمله قرار گرفتن وب‌سایت‌های وردپرس

به گزارش Wordfence، 1.3 میلیون وب‌سایت وردپرس توسط یک کمپین مورد حمله قرار گرفته‌اند. مهاجمان این کمپین سعی دارند با دانلود کردن فایل پیکربندی wp-config.php، نام کاربری و گذرواژه وب‌سایت‌ها را سرقت کنند. از 29 تا 31 ماه می سال جاری، دیوار آتش Wordfence، 130 میلیون حمله روی وب‌سایت‌های وردپرس را شناسایی و مسدود کرده است. این حملات 1.3 میلیون وب‌سایت را هدف گرفته بودند. کاربران نسخه پرمیوم و نسخه رایگان Wordfence در برابر این حمله مصون هستند. در این مدت حملات دیگری نیز روی آسیب‌پذیری‌های افزونه‌ها و تم‌های وردپرس صورت گرفته و حملات این کمپین 75 درصد کل چنین حملاتی را تشکیل می‌دادند. مهاجمانی که این کمپین را اداره می‌کنند، در اواخر ماه آوریل نیز در کمپین دیگری به دنبال سوء استفاده از آسیب‌پذیری‌های XSS وردپرس بودند.

در کمپین قبلی، از 20 هزار IP مختلف برای حمله استفاده می‌شد و در کمپین جدید نیز اکثر حملات با استفاده از همین IPها صورت گرفته‌اند. در حملات اخیر، یک میلیون وب‌سایت جدید نیز مورد هجوم واقع شده‌اند که جزء اهداف کمپین قبلی نبوده‌اند.

در هر دو کمپین، تقریباً تمام حملات، از آسیب‌پذیری‌های قدیمی استفاده می‌کردند که در افزونه‌ها یا تم‌های به‌روز نشده وردپرس وجود دارند. این آسیب‌پذیری‌ها امکان export یا دانلود کردن فایل‌ها را فراهم می‌کنند. در کمپین جدید مهاجمان قصد دانلود فایل wp-config.php را داشتند. این فایل حاوی گذرواژه و اطلاعات اتصال به پایگاه‌داده است و همچنین شامل کلیدهای یکتا و saltهای احراز هویت است. اگر مهاجمی به این فایل دسترسی پیدا کند می‌تواند به پایگاه‌داده وب‌سایت که شامل محتویات وب‌سایت و مشخصات کاربران آن است، دست یابد.

به نظر می‌رسد مهاجمین به طور سیستماتیک کدهای بهره‌برداری را از وب‌سایت exploit-db.com و سایر منابع استخراج و آنها را روی لیستی از وب‌سایت‌ها اجرا می‌کنند. در حال حاضر مهاجمین مشغول استفاده از صدها آسیب‌پذیری هستند، اما آسیب‌پذیری‌های CVE-2014-9734،

CVE-2015-9406، CVE-2015-5468 و CVE-2019-9618 جزء موارد با بیشترین استفاده بوده‌اند.

اگر وب‌سایت شما مورد حمله واقع شده باشد، می‌توانید اثرات آن را در فایل لاگ سرور خود مشاهده کنید. در فایل لاگ به دنبال مدخل‌هایی بگردید که قسمت query آنها شامل wp-config بوده و پاسخ آنها کد 200 است. 10 آدرسی که بیشترین حملات از آنها صورت گرفته عبارت اند از:

- 200.25.60.53
- 51.255.79.47
- 194.60.254.42
- 31.131.251.113
- 194.58.123.231
- 107.170.19.251
- 188.165.195.184
- 151.80.22.75
- 192.254.68.134
- 93.190.140.8

وب‌سایت‌هایی که از Wordfence استفاده می‌کنند در برابر این حملات مصون هستند. اگر از کاربران Wordfence نیستید و احتمال می‌دهید مورد حمله واقع شده باشید، گذرواژه پایگاه داده، کلیدها و saltهای احراز هویت را تغییر دهید. برای ایجاد این تغییرات ممکن است نیاز باشد تا با هاستینگ وب‌سایت خود تماس بگیرید. در ضمن برای جلوگیری از حملات، همه افزونه‌ها و تم‌های وردپرس را به‌روز نگه دارید.

اگر سرور شما طوری پیکربندی شده است که اجازه دسترسی از راه دور را به پایگاه داده می‌دهد، مهاجم با داشتن گذرواژه پایگاه‌داده می‌تواند به راحتی کاربر مدیر جدید اضافه کند، داده‌های حساس را سرقت کند یا کل وب‌سایت را پاک کند. در صورتی که امکان دسترسی از راه دور به پایگاه‌داده فراهم نباشد نیز، ممکن است مهاجم با داشتن کلیدها و saltهای احراز هویت بتواند سایر مکانیزم‌های امنیتی را دور بزند.

منبع خبر :

https://cert.ir/news/13058

Scan Link

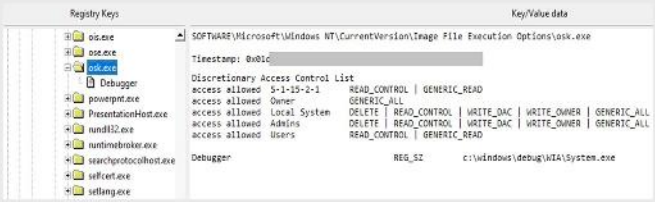
حمله باج‌افزار جدید Tycoon به کاربران ویندوز و لینوکس

کارشناسان امنیتی هشدار داده‌اند که هکرها از یک باج‌افزار مبتنی بر جاوا به نام "Tycoon" برای هدف قرار دادن کاربران ویندوز و لینوکس به منظور قفل کردن فایل‌ها استفاده می‌کنند. این موضوع مشخص است که هکرها به طور مداوم به دنبال روش‌های جدیدی برای حمله به دیتاسنترها و سیستم‌های کاربران عادی برای سرقت داده‌ها و اطلاعات حساس هستند. از آنجا که ویندوز مایکروسافت به عنوان پرکاربردترین سیستم‌عامل شناخته می‌شود به همین دلیل هکرها آن را مورد هدف قرار می‌دهند و همچنین به سیستم‌عامل‌های دیگر مانند macOS و Linux توجه بیشتری دارند.

این باج‌افزار که از اواخر سال 2019 فعالیت خود را آغاز کرده است به زبان جاوا نوشته شده و ویژگی اصلی آن آلوده کردن کاربران ویندوز و لینوکس به یک اندازه است. هکرها Tycoon را درون یک فایل زیپ اصلاح شده پنهان می‌کنند و زمانیکه قربانی آن فایل را باز کرد تروجان اجرا می‌شود. آنها معمولا از سرور RDP و شبکه‌های آسیب‌پذیر استفاده می‌کنند تا به صورت پنهانی وارد سیستم شوند.

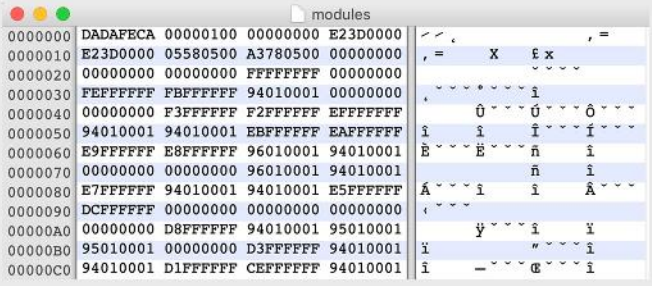
هنگامیه هکر موفق به اجرای باج‌افزار بر روی سیستم قربانی شد، تلاش برای ماندگاری در سیستم را آغاز می‌کند و برای این کار تزریق یک IFEO (Image file execution options) را در عملکرد صفحه کلید روی صفحه نمایش ویندوز انجام می‌دهد.

این باج‌افزار همچنین رمز عبور اکتیودایرکتوری را تغییر داده و آنتی‌ویروس را نیز غیرفعال می‌کند و سپس ابزار کاربردی ProcessHacker hacker-as-a-service را نصب می‌کند. پس از انجام تمام این مراحل، باج‌افزار شروع به رمزگذاری تمام داده‌های موجود در کامپیوتر و درایوهای شبکه می‌کند.



پس از اینکه تمام اقدامات به پایان رسید، باج‌افزار به طور خودکار کلید خصوصی یا private key را برای هکر ارسال می‌کند و سپس این کلید خصوصی را از سیستم قربانی حذف می‌کند و در پایان نیز پیام غافلگیرانه‌ای را به قربانی نمایش می‌دهد.

فایل‌هایی که با باج‌افزار Tycoon رمزگذاری می‌شوند با دو پسوند جدید grinch . و thanos . مشخص می‌شوند.



برای محافظت در برابر این نوع بدافزارها و باج‌افزارها همیشه باید از مهمترین فایل‌های خود نسخه پشتیبان تهیه کنید و همچنین سیستم‌عامل و تمام برنامه‌های نصب شده را همواره بروز نمایید.

جدای از این اقدامات، باید متناسب با سیستم‌عامل خود آنتی‌ویروس مناسب ویندوز یا لینوکس را نصب کنید و در زمان دانلود هر فایل از طریق اینترنت باید مراقب باشید چرا که اکثر آنها حاوی بدافزار هستند.

در ادامه پسوندهای اضافه شده و امضاهای مورد استفاده مهاجمان آورده شده‌اند:

پسورد فایل‌های رمزگذاری شده:

- thanos
- grinch
- redrum

امضاهای فایل‌های رمزگذاری شده:

- happyny3.1
- redrum3_0

منبع خبر :

https://gbhackers.com/tycoon-ransomware/

Scan Link

نقص امنیتی واتس‌اپ و افشای شماره تلفن کاربران در گوگل

اخیراً یک محقق امنیتی به نام Athul Jayaram، به کاربران در خصوص نقص امنیتی موجود در پیام‌رسان واتس‌اپ، موسوم به "Click to Chat" هشدار داد که با اختصاص یک QR code به شماره تلفن کاربر، این امکان را به گوگل می‌دهد تا شماره تلفن‌ها را فهرست کند و به راحتی بتوان آن‌ها را در این موتور جستجو پیدا کرد.

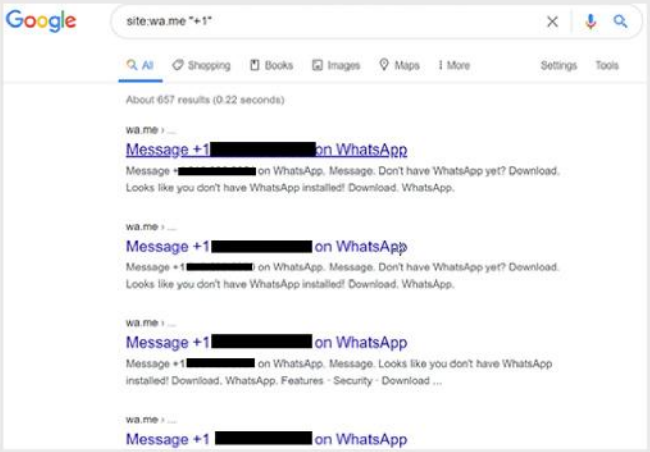
به گفته‌ی وی، این نقص به سایت‌ها اجازه می‌دهد تا به سرعت مکالمات واتس‌اپ را با بازدیدکنندگان خود آغاز کنند، به طوری که بازدیدکننده سایت فقط با اسکن QR code کد یا کلیک بر روی URL و بدون نیازی به وارد کردن شماره تلفن کاربر، گفتگو در واتس‌اپ را آغاز و با شروع مکالمه به شماره تلفن وی دسترسی پیدا کنند.

به گفته‌ی Athul Jayaram، مشکل اینجاست که این شماره تلفن‌ها به گوگل ارجاع داده می‌شوند زیرا موتور جستجو، داده‌های مربوط به "Click to Chat" را فهرست‌بندی کرده و سپس مانند الگوی زیر، شماره تلفن کاربر را در بخشی از URL فاش می‌کند:

(<https://wa.me/<phone_number)

که این مسئله به خودی خود گزینه‌ی پرسودی برای Spammerها به حساب می‌آید، زیرا آن‌ها از طریق این نقص می‌توانند به راحتی پایگاه‌داده‌ی ساخت‌یافته‌ای از شماره تلفن‌های کاربران ایجاد کرده و از آن‌ها برای کمپ‌های مخرب شخصی سوءاستفاده کنند.

علاوه بر این، Athul به صراحت اعلام کرد که موفق شده است به حدود 300,000 شماره تلفن معتبری که در گوگل فهرست شده‌اند، دسترسی پیدا کند. گفتنی است که اگر چه در این فهرست، صاحبان اصلی شماره تلفن‌ها مشخص نمی‌باشد، اما مهاجمان می‌توانند بفهمند که آن‌ها متعلق به چه کسانی هستند.



شکل 1: نمایش شماره تلفن‌های کاربران در موتور جستجوی گوگل

اگر بر روی URL مذکور کلیک کنید، پروفایل کاربر به همراه عکس وی نمایش داده خواهد شد و مهاجم می‌تواند از طریق جستجوی این تصویر، اطلاعات کافی را در خصوص قربانی به دست آورد.

به گفته‌ی Athul Jayaram، در پی گزارش نقص امنیتی به واتس‌اپ، این شرکت آن را رد کرد و این مسئله را به عنوان یک نقص امنیتی نپذیرفت. به گفته سخنگوی واتس‌اپ، کاربران خودشان انتخاب کرده‌اند که شماره تلفن‌های خود را عمومی و فاش کنند. علاوه بر این، آن‌ها شفاف‌سازی کردند که نقص برنامه‌ی bounty، فقط پلت‌فرم‌های Facebook را تحت پوشش خود قرار می دهد، و این در حالیست که واتس‌اپ تنها بخشی از آن به حساب می‌آید. به هر حال وی نظرات خود را در مورد این نقص در فضای مجازی پاک کرد و به شدت به واتس‌اپ تأکید کرد که هر چه سریع‌تر شماره تلفن همه کاربران را رمزگذاری و یک فایل robots.txt را جهت جلوگیری از تجاوز ربات‌ها به دامنه، اضافه کند.

رفع نقص

واتس‌اپ این نقص را پس از گزارش، برطرف و آن را به صورت آنلاین فاش کرد.

به گفته‌ی سخنگوی واتس‌اپ، ویژگی "Click to Chat" در اصل به منظور کمک به کاربران به ویژه شرکت‌های کوچک در سراسر جهان که با مشتریان خود در ارتباط هستند طراحی شده است. وی افزود، ما از تلاش‌ها و وقت صرف شده توسط Athul Jayaram تشکر می‌کنیم اما چون این موضوع تنها حاوی فهرستی از URLها است که به اختیار خود کاربران واتس‌اپ منتشر شده است، لذا مشمول دریافت جایزه نمی‌شود.

تمامی کاربران واتس‌آپ می‌توانند پیام‌های ناخواسته را با فشردن یک دکمه مسدود کنند.

منبع خبر :

https://gbhackers.com/tycoon-ransomware/

Scan Link

آسیب پذیری

آسیب‌پذیری در قابلیت SUBSCRIBE پروتکل UPnP

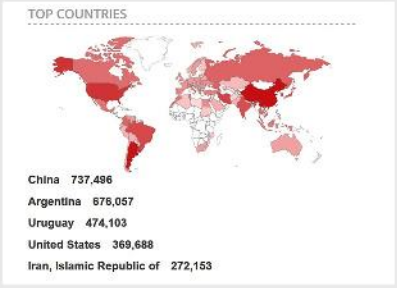
بر اساس گزارشات منتشر شده، پروتکل Universal Plug and Play (UPnP) می‌تواند برای ارسال ترافیک به مقصدهای دلخواه با استفاده از قابلیت SUBSCRIBE مورد سوء استفاده قرار گیرد. این پروتکل به منظور ارائه کشف خودکار و تعامل با دستگاه‌های موجود در شبکه طراحی شده است. پروتکل UPnP به گونه‌ای طراحی شده است که در یک شبکه محلی (LAN) قابل اعتماد مورد استفاده قرار می‌گیرد و هیچ گونه احراز و تصدیق هویت را اجرا نمی‌کند.

بسیاری از دستگاه‌های متصل به اینترنت، از پروتکل UPnP پشتیبانی می‌کنند. آسیب‌پذیری کشف شده در قابلیت UPnP SUBSCRIBE به مهاجمان اجازه می‌دهد تا مقادیر زیادی از داده‌ها را به مقصدهای دلخواه قابل دسترسی از طریق اینترنت ارسال کنند که این امر می‌تواند منجر به حمله Distributed Denial of Service (DDoS)، نشت و سرقت داده‌ها و سایر اعمال غیرمنتظره در شبکه شود. این آسیب‌پذیری با شناسه "CVE-2020-12695" و با عنوان Call Stranger شناخته می‌شود.

آسیب‌پذیری مذکور ناشی از مقدار Callback header در قابلیت UPnP SUBSCRIBE است که توسط یک مهاجم قابل کنترل می‌باشد و یک آسیب‌پذیری شبیه به SSRF را فعال می‌کند.

وضعیت ایران

اگرچه ارائه خدمات UPnP در اینترنت عموماً به عنوان یک پیکربندی اشتباه تلقی می‌شود، اما بر اساس اسکن اخیر موتور جستجوی Shodan، هنوز تعداد زیادی از دستگاه‌ها از طریق اینترنت در دسترس هستند. اسکن اخیر Shodan نشان می دهد که کشور ایران بعد از کشورهای چین، آرژانتین، اروگوئه و ایالات متحده، پنجمین کشوری می‌باشد که سرویس دهندگان UPnP بر روی اینترنت در دسترس می‌باشند و احتمال بهره‌برداری از آسیب‌پذیری ذکر شده بر روی آنها وجود دارد. این گزارش همچنین نشان می‌دهد اکثر تجهیزات مربوط به شرکت‌های ارتباطی مخابرات ایران و برخی از شرکت‌های خصوصی نظیر شاتل و پارس آنلاین می‌باشند. در بین محصولات آسیب‌پذیر نیز نام AvtechAVN801 network camera و Allegro RomPager به چشم می‌خورد. شکل 1 این پراکندگی را نشان می دهد.



شکل 1: میزان پراکندگی دستگاه‌ها با سرویس UPnP در سطح جهان

یک مهاجم غیر مجاز از راه دور ممکن است بتواند از قابلیت UPnP SUBSCRIBE برای ارسال ترافیک به مقصدهای دلخواه خود سوء استفاده کرده و منجر به حملات گسترش‌یافته DDoS و استخراج داده (Exfilteration) شود. به طور کلی، تهیه UPnP از طریق اینترنت می‌تواند آسیب‌پذیری‌های امنیتی بیشتری را نسبت به مواردی که در این گزارش شرح داده شده است، ایجاد کند.

چه کسانی در معرض این آسیب‌پذیری قرار دارند

میلیاردها دستگاه UPNP در شبکه‌های محلی و نیز میلیون‌ها دستگاه UPnP در بستر اینترنت قرار دارند. CallStranger یک آسیب‌پذیری پروتکل است بنابراین تقریبا تمام دستگاه‌های UPnP (و احتمالا دستگاه‌های شما) باید بروزرسانی شوند. شما می‌توانید با استفاده از ابزار موجود در GitHub بررسی کنید که آیا دستگاه شما آسیب‌پذیر است یا خیر.

- **کاربران خانگی**

انتظار نمی‌رود که کاربران خانگی مستقیما مورد هدف قرار گیرند. اگر دستگاه‌های در معرض اینترنت آنها دارای UPnP endpoints باشند، ممکن است دستگاه‌های آنها برای منبع حمله DDoS مورد استفاده قرار گیرند. از ارائه دهنده سرویس‌های اینترنتی (ISP) خود بپرسید که آیا روتر شما در معرض آسیب‌پذیری CallStranger قرار دارد یا خیر.

- **ISP**

ارائه دهندگان سرویس‌های اینترنتی یا ISP ها بـــــه بررسی پشته UPnP روترهای DSL/Cable خود نیاز دارند، از آنها بخواهید که در صورت آسیب‌پذیر بودن قابلیت SUBSCRIBE در دستگاه‌ها، آنها را بروزرسانی نمایند. ISPها می‌توانند دسترسی به پورت‌های شناخته شده‌ی UPnP Control & Eventing را در صورتیکه از طریق اینترنت قابل دسترسی باشند مسدود نمایند. آنها همچنین می‌توانند CPE را با کمک TR-069 مجددا تنظیم کنند.

- **فروشندگان دستگاه**

بسته به مشخصات جدید UPnP در وب‌سایت OCF، باید پشته UPnP دستگاه خود را وصله نمایید. برخی از پشته‌های UPnP مانند miniupnp (بعـــد از سال 2011) آسیب‌پذیر نیستند.

- **شرکت**

ممکن است فروشندگان، وصله دستگاه‌های UPnP را طولانی کنند، شرکت‌ها باید اقدامات خود را انجام دهند. شرکت‌ها باید بسته به رویکرد خود اقدامات لازم را بکار گیرند.

دستگاه‌های آسیب‌پذیر

دستگاه‌هایی که آسیب‌پذیری آنها تایید شده است عبارتند از:

- Windows 10 (All windows versions) - upnphost.dll 10.0.18362.719
- Xbox One- OS Version 10.0.19041.2494
- ADB TNR-5720SX Box (TNR-5720SX-/v16.4-rc-371-gf5e2289 UPnP/1.0 BH-upnpdev/2.0)
- Asus ASUS Media Streamer
- Asus Rt-N11
- Belkin WeMo
- Broadcom ADSL Modems
- Canon Canon SELPHY CP1200 Printer
- Cisco X1000 - (LINUX/2.4 UPnP/1.0 BRCM400/1.0)
- Cisco X3500 - (LINUX/2.4 UPnP/1.0 BRCM400/1.0)
- D-Link DVG-N5412SP WPS Router (OS 1.0 UPnP/1.0 Realtek/V1.3)
- EPSON EP, EW, XP Series (EPSON_Linux UPnP/1.0 Epson UPnP SDK/1.0)
- HP Deskjet, Photosmart, Officejet ENVY Series (POSIX, UPnP/1.0, Intel MicroStack/1.0.1347)
- Huawei HG255s Router - Firmware HG255sC163B03 (ATP UPnP Core)
- NEC AccessTechnica WR8165N Router (OS 1.0 UPnP/1.0 Realtek/V1.3)
- Philips 2k14MTK TV - Firmware TPL161E_012.003.039.001
- Samsung UE55MU7000 TV - Firmware T-KTM-DEUC-1280.5, BT - S
- Samsung MU8000 TV
- TP-Link TL-WA801ND (Linux/2.6.36, UPnP/1.0, Portable SDK for UPnP devices/1.6.19)
- Trendnet TV-IP551W (OS 1.0 UPnP/1.0 Realtek/V1.3)
- Zyxel VMG8324-B10A (LINUX/2.6 UPnP/1.0 BRCM400-UPnP/1.0)

راه‌حل‌ها

- **اعمال بروزرسانی**

توصیه می‌شود تنظیمات به روز شده و ارائه شده توسط OCF پیاده‌سازی شود.

- **غیرفعال یا محدود کردن UPnP**

پروتکل UPnP را در رابط‌های قابل دسترسی به اینترنت غیرفعال کنید. از سازندگان دستگاه خواسته شده است که قابلیت UPnP SUBSCRIBE را در پیـــکربندی پیش‌فرض خود غیرفعال کنند و از کاربران بخواهند تا صریحا با محدودیت‌های مناسب شبکه، SUBSCRIBE را فعـــال کنند تا میزان استفاده آن از یـــک شبکه محلی قابل اعتماد محدود شود.

- **IDS Signature**

مدیران شبکه و ISPها می‌توانند یک signature را در تجهیزات لبه اتصال شبکه سازمان خود به اینترنت تعریف نمایند تا هرگونه درخواست غیرعادی SUBSCRIBE که به کاربرانشان می‌رسد را تشخیص دهند. به عنوان مثال امضای زیر برای IDS Surricata قابل استفاده می‌باشد:

```
alert http any any -> ![fd00::/8,192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]
any (msg:"UPnP SUBSCRIBE request seen to external network VU#339275:
CVE- 2020-12695 https://kb.cert.org"; content:"subscribe"; nocase; http_met
hod; sid:1367339275;)
```

جمع بندی

درنهایت با توجه به اینکه این آسیب‌پذیری مربوط به یک پروتکل می باشد، زمان زیادی نیاز دارد که اصلاح و رفع شود. در حال حاضر پیشنهاد می گردد این آسیب‌پذیری را جدی گرفته و تا رفع کامل آن، سرویس UPnP را محدود و یا مسدود سازید. با توجه به گستردگی و اهمیت موضوع، پیشنهاد می‌شود کلیه مدیران و کارشناسان فناوری اطلاعات علی الخصوص شرکت‌های مذکور هر چه سریعتر نسبت به بررسی تنظیمات تجهیزات خود و مشتریانشان اقدام لازم را انجام دهند.

منبع خبر :

https://callstranger.com/

Scan Link

آسیب‌پذیری بحرانی در Sign in اپل

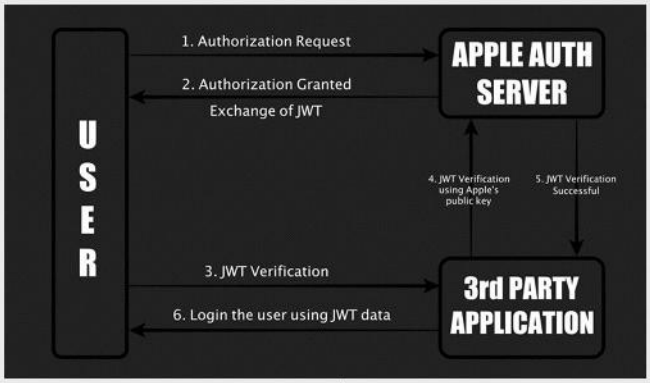
شرکت اپل به تازگی جایزه 100،000 دلاری خود را برای گزارش یک آسیب‌پذیری بحرانی در Sign in اپل، به یک محقق آسیب‌پذیری هندی به نام Bhavuk Jain پرداخت کرد.

این آسیب‌پذیری امکان احراز هویت از راه دور را برای مهاجمان فراهم آورده و حساب‌های کاربری موردنظر بر روی سرویس‌های third-party و نیز اپلیکیشن‌هایی که از طریق Sign in اپل رجیستر شده‌اند را هدف قرار می‌دهد.

سال گذشته در کنفرانس WWDC اپل، ویژگی Sign in به عنوان مکانیسمی جهت حفظ حریم خصوصی کاربران، به جهانیان معرفی شد تا از طریق اپلیکیشن‌های 3rd-party و بدون افشای آدرس ایمیل واقعی، یک حساب کاربری را ثبت کنند(همچنین به عنوان Apple ID نیز مورد استفاده قرار می‌گیرد).

Bhavuk Jain در مصاحبه‌ای با هکرنیوز اذعان داشت که با وجود این آسیب‌پذیری، تصدیق هویت کاربر، پیش از درخواست از سرورهای احرازهویت اپل، امکان‌پذیر است. سرور ضمن تصدیق هویت کاربر از طریق Sign in اپل، یک JWT[1] را تولید می‌کند که حاوی اطلاعات محرمانه‌ای است که اپلیکیشنِ third-party جهت تصدیق هویت کاربر هنگام ورود به سیستم از آن‌ها استفاده می‌کند.

Bhavuk دریافت که اگرچه اپل پیش از بررسی یک درخواست، از کاربران می‌خواهد به حساب کاربری خود وارد شوند، اما در واقع اگر همان شخص JWT را در مرحله‌ی بعدی از سرور احراز هویت خود در خواست کند، این امر (یعنی ورود به حساب کاربری اپل) نامعتبر می‌باشد.



مراحل آسیب‌پذیری

بنابراین اعتبارسنجی از دست رفته در این بخش از مکانیسم، می‌تواند این امکان را به مهاجم دهد تا یک Apple ID مجزا که متعلق به فرد قربانی است را ایجاد کند و از این طریق سرورهای اپل را فریب داده و پی‌لود JWT را جهت ورود به سرویس 3rd-party، با هویت متعلق به قربانی تولید کند.

Bhavuk افزود: "من می‌توانم JWT را برای هر شناسه‌ی ایمیل[2] از اپل درخواست کنم تا هنگامی که این توکن‌ها از طریق کلید عمومی اپل تأیید شدند، معتبر شناخته شوند، این بدان معناست که یک مهاجم می‌تواند با لینک کردن هر شناسه‌ی ایمیل و دسترسی به حساب قربانی، JWT را جعل کند."وی در ادامه افزود حتی اگر بخواهید شناسه‌ی ایمیل خود را از سرویس‌های rd-party3 مخفی کنید، این آسیب‌پذیری می‌تواند برای ثبت یک حساب کاربری جدید با Apple ID قربانی اکسپلویت شود."

این آسیب‌پذیری بسیار مهم می‌باشد چرا که از طریق آن می‌توان حساب کاربری را به طور کامل تصاحب کرد. بسیاری از توسعه‌دهندگان، Sign in اپل را ادغام کرده اند، زیرا این امر برای اپلیکیشن‌هایی که از سایر ورودهای اجتماعی[3] پشتیبانی می‌کنند الزامی می‌باشد، مانند Dropbox, Spotify, Airbnb و Giphy.

Bhavuk بیان کرد که اگرچه این آسیب‌پذیری در سمت کد اپل وجود دارد اما بسیاری از سرویس‌ها و اپلیکیشن‌های ارائه شده با Sign in اپل، قبلاً از احراز هویت دو مرحله‌ای استفاده کرده‌اند که این امر می‌تواند خطر را برای کاربران کاهش دهد.

Bhavuk در ماه گذشته این موضوع را به تیم امنیتی اپل گزارش داد و این شرکت نیز آسیب‌پذیری مذکور را برطرف کرد.

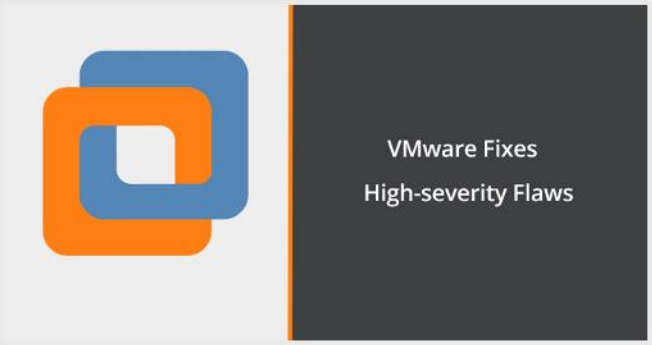
[1] JSON Web Token
[2] Email ID
[3] social logins

منبع خبر :

https://bit.ly/37scatT

Scan Link

وصله چند آسیب‌پذیری با شدت بالا در محصولات VMware



بر اساس گزارشات منتشر شده، VMware چند آسیب‌پذیری با شدت بالا را وصله کرده است که بر روی چندین محصول این شرکت تاثیر می‌گذارد و بهره‌برداری از آنها به مهاجمان اجازه می‌دهد تا به اطلاعات حساس دست یابند.

شرح آسیب‌پذیری‌ها

- **CVE-2020-3960**

یکی از آسیب‌پذیری‌های وصله شده که با شناسه "CVE-2020-3960" شناخته می‌شود، یک آسیب‌پذیری خواندن out-of-bounds می‌باشد که VMware ESXi، Workstation و Fusion را تحت تاثیر قرار می‌دهد. به کاربران توصیه می‌شود که نرم‌افزارهای فوق را به نسخه‌های وصله شده بروز نمایند.

این نقص در عملکرد NVMe قرار دارد. NVMe (nonvolatile memory express) یک پروتکل جدید دسترسی به storage و انتقال برای فلش و SSDs است که بالاترین توان و سریعترین زمان پاسخگویی را برای تمام حجم کاری سازمان ارائه می‌دهد.

به موجب این آسیب‌پذیری، مهاجم با دسترسی لوکال و non-administrative به یک ماشین مجازی، ممکن است بتواند اطلاعات ویژه و خاص موجود در حافظه را بخواند.

محصولات آسیب‌پذیر و وصله شده برای آسیب‌پذیری CVE-2020-3960

Product	Version	Running On	CVE Identifier	CVSS v3	Severity	Fixed Version	Workarounds	Additional Documentation
ESXi	7.0	Any	CVE-2020-3960	N/A	N/A	Unaffected	N/A	N/A
ESXi	6.7	Any	CVE-2020-3960	7.1	Important	ESXi670-202006401-SG	None	None
ESXi	6.5	Any	CVE-2020-3960	7.1	Important	ESXi650-202005401-SG	None	None
Workstation	15.x	Any	CVE-2020-3960	7.1	Important	15.5.5	None	None
Fusion	11.x	Any	CVE-2020-3960	7.1	Important	11.5.5	None	None

- **CVE-2020-3961**

نقص بعدی یک آسیب‌پذیری ارتقاء سطح دسترسی است که در VMware Horizon Client مربوط به سیستم‌عامل ویندوز وجود دارد و ناشی از پیکربندی مجوزهای دسترسی و بارگزاری ناامن کتابخانه‌ها می‌باشد.

آسیب‌پذیری مذکور می‌تواند توسط یک کاربر لوکال در سیستم، مورد سوءاستفاده قرار گیرد و پس از آن به عنوان هر کاربر دیگری دستورات را اجرا نماید.

این آسیب‌پذیری بر روی Horizon Client 5.x مخصوص ویندوز تاثیر می‌گذارد و پیش از این، در نسخه 5.4.3 وصله شده است. به این آسیب‌پذیری شدت important و CVSSv3 8.4 اختصاص داده شده است.

محصولات آسیب‌پذیر و وصله شده برای آسیب‌پذیری CVE-2020-3961

Product	Version	Running On	CVE Identifier	CVSS v3	Severity	Fixed Version	Workarounds	Additional Documentation
Horizon Client for Windows	5.x and prior	Windows	CVE-2020-3961	8.4	Important	5.4.3	None	None

- **CVE-2020-3956**

آسیب‌پذیری بعدی یک آسیب‌پذیری تزریق کد در VMware Cloud Director است که منجر به اجرای کد از راه دور می‌شود. این آسیب‌پذیری می‌تواند با ارسال ترافیک مخرب به VMware Cloud Director و از طریق HTML5 و Flex-based API Explorer interface، UIs و دسترسی API مورد اکسپلویت قرار گیرد.

VMware Cloud Director یک بستر ارائه‌دهنده خدمات ابری است که به سازمان‌ها امکان می‌دهد تا کسب و کارهای سرویس ابری را مدیریت و اجرا کنند.

این آسیب‌پذیری به طور بالقوه می‌تواند به یک مهاجم احراز هویت شده امکان دسترسی به شبکه شرکت‌ها، دسترسی به داده‌های حساس و کنترل فضای ابری محرمانه را در تمام زیرساخت‌ها فراهم کند.

محصولات آسیب‌پذیر و وصله شده برای آسیب‌پذیری CVE-2020-3956

Product	Version	Running On	CVE Identifier	CVSS V3	Severity	Fixed_Version	Workarounds	Additional Documentation
VMware Cloud Director	10.1.0	Linux, Photon OS appliance	CVE-2020-3956	N/A	N/A	Not affected	N/A	N/A
vCloud Director	10.0.x	Linux, Photon OS appliance	CVE-2020-3956	8.8	Important	10.0.0.2	KB79091	None
vCloud Director	9.7.x	Linux, Photon OS appliance	CVE-2020-3956	8.8	Important	9.7.0.5	KB79091	None
vCloud Director	9.5.x	Linux, Photon OS appliance	CVE-2020-3956	8.8	Important	9.5.0.6	KB79091	None
vCloud Director	9.1.x	Linux	CVE-2020-3956	8.8	Important	9.1.0.4	KB79091	None
vCloud Director	9.0.x	Linux	CVE-2020-3956	N/A	N/A	Not affected	N/A	N/A
vCloud Director	8.x	Linux	CVE-2020-3956	N/A	N/A	Not affected	N/A	N/A

راه‌حل

با توجه به اهمیت آسیب‌پذیری‌های ذکر شده و نیز عمومیت استفاده از نرم‌افزارهای فوق، توصیه می‌شود کاربران هر چه سریعتر نسبت به بروزرسانی محصولات آسیب‌پذیر اقدام نمایند.

منبع خبر :

https://bit.ly/2YvfKPO

Scan Link

آسیب‌پذیری جدید StrandHogg ۲,۰ در اندروید

Strandhogg 2.0 Affects all Devices Running Android 9.0 and Earlier

آسیب‌پذیری جدید اندروید به نام StrandHogg 2.0، بر روی تمام دستگاه‌های دارای Android 9.0 و نسخه‌های قبل‌تر از آن تاثیر می‌گذارد. این باگ به اپلیکیشن‌های مخرب اجازه می‌دهد تا در قالب یک اپلیکیشن مجاز، داده‌های قربانی را سرقت کند.

این آسیب‌پذیری که توسط محققان Promon و شناسه "CVE-2020-0096" ردیابی شده است شبیه به باگ اصلی StrandHogg است که سال گذشته کشف شده بود.

برنامه StrandHogg 2.0 به مهاجمان امکان می‌دهد که تقریبا تمام اپلیکیشن‌ها را ربوده و داده‌های حساس کاربر مانند مخاطبین و عکس‌ها را دریافت کرده و موقعیت مکانی قربانی را ردیابی کنند.

با استفاده از StrandHogg 2.0، اگر یک برنامه مخرب بر روی دستگاه نصب شده باشد به مهاجمان اجازه می‌دهد تا دسترسی به پیامک‌ها و عکس‌های محرمانه را بدست آورند، اطلاعات ورود قربانیان را به سرقت برند، تغییرات GPS را ردیابی کنند، مکالمات تلفنی را دریافت و یا ضبط کنند و از طریق دوربین گوشی و میکروفون به جاسوسی بپردازند.

برای بهره‌برداری از این آسیب‌پذیری، دسترسی root مورد نیاز است.

در این تحقیق آمده است: با بهره‌برداری از این آسیب‌پذیری یک برنامه مخرب نصب شده بر روی دستگاه می‌تواند به کاربر حمله کرده و او را فریب دهد به طوریکه با کلیک بر روی آیکون یک برنامه مجاز، یک نسخه مخرب به جای آن در صفحه کاربر، نمایش داده می‌شود.

اگر قربانیان اطلاعات ورود و داده‌های حساس را با برنامه مخرب وارد کنند، جزئیات آن به سرور مهاجم ارسال می‌شود.

بدافزارهایی که از StrandHogg 2.0 بهره‌برداری می‌کنند حتی توسط اسکنرهای امنیتی و آنتی‌ویروس‌ها نیز قابل شناسایی نیستند. براساس داده‌های گوگل در آوریل 2020، 91.8 درصد از کاربران اندروید از نسخه 9.0 یا قبل‌تر از آن استفاده می‌کنند.

کاربران اندوریدی برای محافظت از حمله Strandhogg 2.0، باید در اسرع وقت سیستم‌عامل خود را به جدیدترین نسخه بروزرسانی کنند.

منبع خبر :

https://gbhackers.com/strandhogg-2-0/

Scan Link

اخبار کوتاه

آسیب‌پذیری CrossTalk نشت اطلاعات از پردازنده‌های اینتل را ممکن می‌کند

محققان امنیتی دانشگاه «وریج» هلند (Vrije University Group) آسیب‌پذیری جدیدی به نام «CrossTalk» در پردازنده‌های اینتل کشف کرده‌اند که هکرها به کمک آن می‌توانند با اجرای کد مخرب روی یکی از هسته‌های CPU، اطلاعات حساس برنامه‌هایی که روی هسته دیگر در حال اجرا شدن هستند را نشت کنند.

محققان می‌گویند آسیب‌پذیری CrossTalk نوع دیگری از حمله MDS است که در آن داده‌های کاربر حین پردازش در پردازنده هدف گرفته می‌شوند. حمله CrossTalk به طور خاص داده‌هایی که توسط کش LBF در حال پردازش هستند را هدف قرار می‌دهد.

محققان می‌گویند از سپتامبر 2018 به منظور رفع آسیب پذیری CrossTalk در حال همکاری با اینتل بوده‌اند. به گفته آن‌ها پچ کردن این آسیب‌پذیری به دلیل پیچیدگی و عدم آگاهی آن‌ها از امکان نشت اطلاعات از هسته‌های پردازنده، بیشتر از مدت زمان استاندارد یعنی 90 روز زمان برده است.

اینتل نیز در این مدت بیکار ننشسته و تغییرات قابل توجهی را در طراحی پردازنده‌های خود ایجاد کرده است و بیشتر CPUهای جدید این شرکت در برابر این حمله آسیب‌پذیر نیستند.

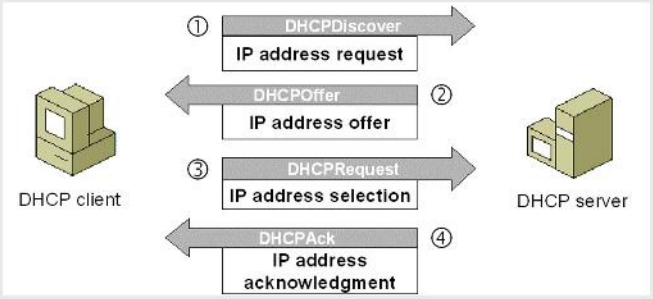
این تراشه ساز برای پردازنده‌های قدیمی به روزرسانی نرم‌افزاری منتشر کرده که آسیب پذیری CrossTalk را رفع می‌کند.

اینتل از آسیب‌پذیری CrossTalk با نام «SRBDS» یاد کرده و با انتشار بیانیه‌ای می گوید از آن در بیرون از محیط آزمایشگاه سوءاستفاده‌ای نشده است.

مقالات آموزشی

حمله DHCP Spoofing و راهکار مقابله با آن در سیسکو

پروتکل DHCP یکی از پروتکل‌های مدل TCP/IP می‌باشد که در لایه application مورد استفاده قرار می‌گیرد و توسط سازمان IETF تحت RFC 2131 و RFC 3396 معرفی شده است. DHCP که مخفف کلمات Dynamic Host Configuration Protocol می‌باشد یک پروتکل ارتباطاتی است که مدیران شبکه را قادر به مدیریت مرکزی و اتوماتیک IP address ها در شبکه می‌کند.



مراحل اختصاص IP از DHCP Server به کلاینت

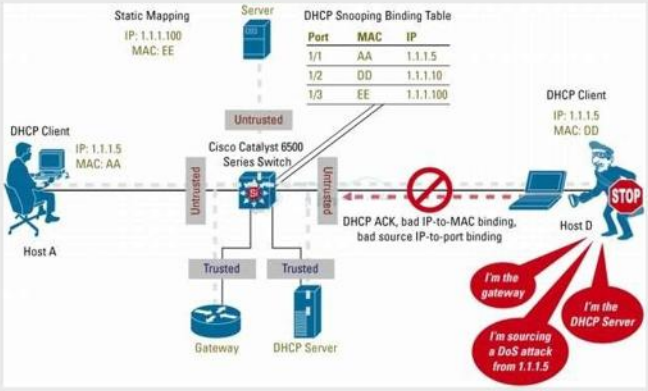
سرویس DHCP یکی از مهمترین سرویس‌هایی است که در یک شبکه ارائه می‌شود، از حملاتی که ممکن است روی این سرویس رخ دهد حمله DHCP Spoofing است.

DHCP Spoofing حمله‌ای است که عملکرد سرویس (اختصاص IP به صورت اتومات) را مختل می‌کند.

این حمله به دو صورت می‌تواند به وجود آید:

1) DHCP Server Spoofing: در این نوع از حمله، مهاجم به بسته‌های DHCP Request گوش می‌کند و بلافاصله به آنها جواب می‌دهد و IP Address و مشخصات مورد نظر خود را برای قربانی ارسال می‌کند به این نوع حملات man in the middle گفته می‌شود. به طور مثال IP خود را به عنوان Gateway به قربانی اعلام می‌کند در نتیجه قربانی بسته‌هایی که مقصد آنها خارج از شبکه هستند را به مهاجم تحویل می‌دهد و مهاجم اطلاعات مورد نظر خود را از این بسته استخراج می‌کند و سپس بسته را به سوی مقصد واقعی ارسال می‌کند و قربانی از این اتفاق بی اطلاع است.

2) DHCP Starvation: حالت دوم حمله جهت از کار انداختن سرویس DHCP مورد استفاده قرار می‌گیرد به این صورت که مهاجم تعداد زیادی DHCP Request جعلی ایجاد می‌کند و باعث می‌شود که کل محدود IP تعیین شده برای DHCP سرور پر شود یا تعداد این DHCP Request به اندازه‌ای زیاد می‌شود که سرور توان پاسخگویی به آن را نداشته باشد.



راهکار جلوگیری از حمله DHCP Snooping

1) به منظور جلوگیری از حمله DHCP Server Spoofing پورتی که متصل به DHCP سرور است را بایستی به عنوان Trust معرفی کنیم این کار سبب می‌شود تنها پورت Trust شده اجازه داشته باشد به بسته‌های DHCP Request پاسخ دهد.

2) برای جلوگیری از حمله DHCP Starvation باید برای پورت مشخص کنید که در هر ثانیه اجازه دارد چند پیغام DHCP Request را دریافت کند. و یا بایستی مکانیزم Port Security را روی دستگاه پیکربندی نمایید.

نکته: در صورتی که DHCP سرور روی سوئیچ فعال باشد حمله DHCP Server Spoofing رخ نخواهد داد.

اخبار کوتاه

رمزگشای باج‌افزار جعلی از آب درآمد؛ Zorab مشکل قربانیان را دوچندان می‌کند

زمانی که یک باج‌افزار فایل‌های شما را گروگان بگیرد، در اینترنت به دنبال راه‌حلی برای آن می‌گردید تا بدون پرداخت هزینه بتوانید اطلاعات را پس بگیرید. اگرچه اغلب این کار بی‌نتیجه است اما همین موضوع باعث شده مهاجمان یک رمزگشای باج‌افزار جعلی با نام «Zorab» درست کنند.

مهاجمان سایبری تصمیم گرفتند که با رمزگشای خود مشکلات کاربرانی که با باج‌افزار «STOP/Djvu» دست و پنجه نرم می‌کنند را افزایش دهند. این باج‌افزار انواع مختلفی دارد که تمام آن‌ها اطلاعات را رمزگذاری می‌کنند. حالا رمزگشای Zorab بجای اینکه اطلاعات کاربران را به پس بگیرد، آن‌ها را دوباره رمزگذاری می‌کند.

یکی از موارد مهم، شناسایی جعلی بودن یک رمزگشا است. اگر فردی بتواند باج‌افزارهای شناخته شده را رمزگشایی کند، مسلما ابزار آن را در یک سایت ناشناخته قرار نمی‌دهد یا لینک‌های دریافت آن را به صورت مستقیم در شبکه‌های اجتماعی یا فروم‌ها قرار نمی‌دهد. این ابزارها معمولا توسط شرکت‌های مطرح توسعه پیدا می‌کنند و در وب‌سایت‌های مطرح قرار می‌گیرند.

برای جلوگیری از دچار شدن به باج‌افزارها از باز کردن لینک‌های مشکوک یا اجرای برنامه‌هایی که از سازنده‌ها آن‌ها شناختی ندارید، جلوگیری کنید و همواره از فایل‌های مهم خود نسخه پشتیبان تهیه کنید.

واقعیت تاریک دنیای متن باز؛ تعداد آسیب‌پذیری‌ها بیش از ۲ برابر شده است

تحقیق جدید شرکت «RiskSense» نشان می‌دهد که تعداد آسیب‌پذیری‌های نرم افزارهای متن باز نسبت به سال گذشته میلادی، بیش از دو برابر شده است.

برای تهیه این گزارش که عنوان «واقعیت تاریک دنیای متن باز» را یدک می‌کشد، شرکت از اطلاعات 54 پروژه متن باز از سال 2015 تا فصل اول 2020 استفاده کرده که نتیجه آن، کشف 2694 مورد آسیب‌پذیری یا تهدید امنیتی منحصر به فرد (CVE) بوده است.

بر اساس این تحقیق، تعداد آسیب‌پذیری‌ها در نرم افزارهای متن باز در سال گذشته به 968 مورد رسیده که افزایشی چشمگیری را نسبت به 421 آسیب‌پذیری در سال 2018 تجربه کرده است. مدیرعامل این شرکت امنیتی، «Srinivas Mukkamala» اطلاعات بیشتری پیرامون این گزارش به اشتراک گذاشته است:

"در حالی که اغلب مواقع امنیت کد متن باز بالاتر از نرم افزارهای تجاری درنظر گرفته می‌شود، تحقیق اخیر نشان می‌دهد که تعداد آسیب‌پذیری‌ها در این نرم افزارها افزایش چشمگیری داشته و می‌تواند برای بسیاری از سازمان‌ها به عنوان نقطه کور تلقی شود. از آنجایی که نرم افزارهای متن باز به صورت روزانه مورد استفاده قرار می‌گیرند، زمانی که آسیب‌پذیری‌ها کشف می‌شوند، می‌توانند عواقب بسیار سنگینی داشته باشند."

ابزار جدید IBM امنیت داده‌ها را در اندروید و iOS دو چندان می‌کند

ابزار جدید IBM امکان دسترسی آسانتر توسعه دهندگان به فناوری رمزنگاری تمام همریخت را فراهم می‌سازد که از داده‌های حساس در برابر حملات سایبری حفاظت می‌کند. رمزنگاری داده‌ها یکی از راه‌های حراست از آنها در برابر حملات سایبری و شنود پنهانی است. داده‌ها معمولا زمانی که ذخیره شده یا در حال انتقال هستند، رمزنگاری می‌شوند اما رمزگشایی آنها در زمان استفاده فرصتی را برای دسترسی به اطلاعات در اختیار هکرها قرار می‌دهد.

IBM یازده سال قبل برای حل این مشکل فناوری رمزنگاری تمام هومومورفیک یا همریخت (FHE) را معرفی کرد که امکان محاسبه و پردازش داده‌ها بدون نیاز به رمزگشایی را فراهم می‌کرد. رمزنگاری تمام همریخت با کاهش چشمگیر دفعات رمزگشایی خطر افشای اطلاعات به ویژه برای اطلاعات حساس را به حداقل رساند اما مشکل اصلی پیچیدگی بالای پیاده سازی این تکنیک در برنامه‌ها بود و به همین خاطر کمپانی آمریکایی با معرفی یک ابزار جدید استفاده از آن را برای توسعه‌دهندگان تسهیل کرده است.

مزیت اصلی رمزنگاری تمام همریخت برای صنایع و سازمان‌هایی است که با داده‌های محرمانه و بسیار ارزشمند نظیر پرونده‌های مالی یا سلامتی سر و کار دارند. این فناوری امکان به اشتراک گذاری داده‌ها، استفاده از آنها و ذخیره سازی با امنیت به مراتب بالاتر را میسر می‌سازد.

ابزار جدید IBM برای iOS و MacOS در گیت هاب ارائه شده و طی چند هفته بعد نسخه‌های ویندوز و لینوکس آن هم از راه می‌رسند. تمامی نسخه‌ها مبنی بر غنی‌ترین کتابخانه رمزنگاری یعنی HELib هستند.

امنیت کاربر رایانه

امنیت شبکه های اجتماعی

این روزها حضور درشبکه‌های اجتماعی بسیار زیاد شده است افراد مختلف با سن، تحصیلات، جنسیت و شغل‌های مختلف در این شبکه‌ها عضو هستند و کاربران روزانه میلیون‌ها بار به انتشار مطالب مختلف اقدام می‌کنند و از این رو امنیت شبکه‌های اجتماعی ضرورت یافته است. اما همانطور که در زندگی واقعی انسان‌ها می‌بایست قوانین و آدابی را رعایت کنند زندگی در چنین فضای مجازی و شبکه‌های اجتماعی نیز آدابی دارد که بایستی به آنها توجه ویژه‌ای کرد تا کمتر آسیب ببینیم و از بروز مشکلات جدی جلوگیری شود.

حال با توجه به اهمیت این موضوع، در این شماره از بولتن خبری به بیان "راهکارهای افزایش امنیت در شبکه‌های اجتماعی" می‌پردازیم.

با ما همراه باشید...

مزایای شبکه های اجتماعی :

بسیاری از شرکت‌های فعال در زمینه فناوری اطلاعات (IT) دسترسی کارمندان خود به شبکه‌های اجتماعی همانند خارجی از قبیل تلگرام و فیس‌بوک را بسته و تحت هیچ شرایطی اجازه ورود کارمندان به شبکه‌های اجتماعی را نمی‌دهند اما این راه‌حل امروزه در این شرایط جهانی کمی سخت گیرانِ به نظر می‌رسد. بسیاری از شرکت‌های اینترنتی نیاز به استفاده از **شبکه‌های اجتماعی به‌عنوان یک بستر فروش و بازار بزرگی جهت تبلیغات محصولات خود** هستند بنابراین مسئولان و مدیران IT سازمان می‌بایست راهکارهای هوشمندانه‌تری را انتخاب کنند .

۸ راه کار کلی امنیتی :

۱- محدود کردن اطلاعاتی که پست می‌کنید

۲- مراقب بیگانه‌ها باشید

۳- شکاک باشید

۴- پسوردهای قوی انتخاب کنید

۵. تنظیمات خود را بازبینی نمایید

۶. مراقب اپلیکیشن های شخص ثالث باشید

۷. مرورگر خود را به‌روز نگه‌دارید

۸.خط‌مشی محرمانگی وب سایت‌ها را چک کنید

۱- محدود کردن اطلاعاتی که پست می‌کنید:

اطلاعاتی که ممکن است برایتان دردسر شود مانند **آدرس یا برنامه‌های روزانه‌تان** ازجمله اطلاعات محرمانه شما هستند اگر دوستان و اطرافیانتان اطلاعاتی از شما پست کرده‌اند مطمئن شوید در حدی باشد که آگاهی غریبه‌ها از آن مشکل‌ساز نشود همچنین به اطلاعاتی که خود از اطرافیانتان پست می‌کنید هم توجه داشته باشید همیشه به یاد داشته باشید که **اینترنت مکانی عمومی** است فقط اطلاعاتی را پست کنید که با دیده و یا خوانده شدن آن مشکلی نداشته باشید.

۲- مراقب بیگانه‌ها باشید:

اینترنت تغییر هویت را برای افراد ساده کرده است. تعداد افرادی که می‌توانند با شما ارتباط داشته باشند محدود کنید اگر باکسی که او را نمی‌شناسید ارتباط دارید مراقب میزان اطلاعاتی که آشکار می‌سازید و قرارهایی که می‌گذارید باشید.

۳- شکاک باشید:

هر آنچه آنلاین می‌بینید و می‌خوانید را باور نکنید. افراد می‌توانند اطلاعات نادرست یا جهت‌داری را در موضوعات مختلف مانند هویتشان پست کنند هرچند ممکن است عامدانه نبوده و اغراق و یا حتی شوخی باشد به هر صورت مراقب باشید و به منبع و موثق بودن اطلاعات خود مطمئن باشید پیش از آنکه دست‌به‌کاری بزنید.

۴- پسوردهای قوی انتخاب کنید:

برای تمامی اکانت های خود پسورد پیچیده انتخاب کنیدکه نتوان به‌راحتی آن را حدس زد. اگر رمزهای شما ساده باشند دیگران و افراد هکر به‌راحتی می‌توانند به رمزها دست‌یافته و خود را به‌جای شما جا بزنند پسورد پیچیده می‌بایست شرایط زیر را داشته باشد:

۱-ترجیحاً از ۱۰ کاراکتر به بالا تشکیل‌شده باشد

۲-شامل حروف کوچک باشد

۳-شامل حروف بزرگ باشد

۴-شامل علامت باشد مانند *&٪$#@

۵. تنظیمات خود را بازبینی نمایید:

از تنظیمات محرمانگی سایت‌ها نهایت بهره را ببرید. تنظیمات پیش‌فرض برخی تارنماها امکان دیده شدن مطالب شمارا به دیگران می‌دهد اما شما می‌توانید با تغییر کوچکی آن را محدود به افراد خاصی بکنید بااین‌همه بازهم ممکن است اطلاعات شما دیده شود پس حواستان باشد که چه اطلاعاتی را آشکار می‌کنید ممکن است سایت‌ها به‌طور منظم آپشن های خود را تغییر دهند پس تنظیمات امنیتی خود را مرتباً بازبینی نمایید تا از درست بودن آن‌ها اطمینان حاصل نمایید.

۶. مراقب اپلیکیشن های شخص ثالث باشید:

این اپلیکیشن ها برنامه‌های کاربردی و سرگرمی را برای کاربران فراهم می‌کنند اما مراقب باشید چه نرم‌افزاری را فعال می‌کنید. **از برنامه‌های مشکوک بپرهیزید و تنظیمات خود را برای محدود کردن مقدار اطلاعاتی که برنامه‌ها به آن دسترسی دارند تغییر دهید.**

۷. مرورگر خود را به‌روز نگه‌دارید:

همواره **تمامی نرم‌افزارهای خود را به‌روز نگه‌دارید** تا هکرها نتوانند از ضعف مای امنیتی به شما ضربه بزنند توصیه می‌شود که سیستم‌های عامل خود را آپدیت نمایید و این قابلیت را فعال نگه‌دارید.

۸.خط‌مشی محرمانگی سایت‌ها را چک کنید:

برخی سایت هااطلاعات و ایمیل کاربران را با سایت های دیگر به اشتراک می‌گذارند و در مواقعی شاهد هستیم که **اطلاعات شمارا به فروش می‌رسانند** که به افزاش spam یا هرزنامه منجر می‌شود. لذا ارجاعات خود را بازبینی کنید تا از فرستاده شدن اسپم به دوستان خود جلوگیری کنید برخی سراچه‌ها ارسال ایمیل به دوستان شمارا تا زمانی که به آن‌ها بپیوندند ادامه می‌دهند.

اخبار داخلی

وبینار رایگان امنیت در درگاه‌های بانکی

امروزه با همه گیر شدن اینترنت در میان مردم و در پیرو آن به وجود آمدن پرداخت‌های الکترونیکی و همچنین فروشگاه‌های اینترنتی که کالاهایی اعم از کالاهای حقیقی و مجازی را در قبال پرداخت وجه در اختیار مصرف کنندگان قرار می‌دهند، به طبع آن کلاهبرداری در فضای مجازی بوجود آمده است. از همین رو مرکز تخصصی آپا دانشگاه رازی در راستای انجام رسالت خویش در زمینه آگاهی‌رسانی، در جهت بیان نکات و موارد امنیتی با هدف به حداقل رساندن کلاهبرداری در فضای مجازی، وبینار رایگان امنیت در درگاه‌های بانکی را در تاریخ ۲ خرداد با حضور آنلاین دانشجویان ، پرسنل سازمان‌ها، شرکت‌ها و علاقمندان برگزار کرد.

وبینار رایگان مقابله با ویروس‌های باج‌افزاری

باج‌افزارها (Ransomware) گونه‌ای از بدافزارها هستند که دسترسی به سیستم را محدود می‌کنند و ایجادکننده آن برای برداشتن محدودیت درخواست باج می‌کند. برخی از انواع آن‌ها روی فایل‌های هارددیسک رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سیستم را قفل کنند و پیام‌هایی روی نمایشگر نشان دهند که از کاربر می خواهد مبالغی را واریز کنند. برخی از این بد افزارها در صورتی که در زمان مشخص شده مبلغ درخواستی پرداخت نگردد مبالغ پرداختی را افزایش می‌دهند مرکز تخصصی آپا دانشگاه رازی نکات و موارد امنیتی جهت جلوگیری از آلوده شدن سیستم‌ها به باج افزارها را در قالب وبینار مقابله با ویروس های باج افزاری در مورخه ۲۲ خرداد با حضور آنلاین علاقمندان برگزار کرد.

اخبار کوتاه

افزایش دو برابری برنامه‌های اندرویدی مخرب در فصل اول ۲۰۲۰ به دلیل کرونا

بر اساس گزارشی جدید، ده‌ها هزار اپلیکیشن مخرب اندرویدی میلیون‌ها کاربر این سیستم‌عامل را در معرض خطر حملات سایبری و کلاهبرداری اینترنتی قرار داده‌اند.

شرکت امنیتی «Upstream» در ماهه اول 2020، بیش از 29 هزار اپلیکیشن اندرویدی مخرب را شناسایی کرده که کاربران همچنان از آن‌ها استفاده می‌کنند. این آمار نسبت به تعداد اپلیکیشن‌های فعال مخرب در مدت زمان مشابه در سال قبل (14 هزار و 500)، دو برابر شده است.

این شرکت در تحقیقات خود دریافت که 9 مورد از مخرب‌ترین اپلیکیشن‌ها همچنان در پلی استور برای دانلود در دسترس هستند. به گفته این شرکت چنین آماری نشان می‌دهد هکرها همواره روش‌هایی برای دور زدن سیستم‌های امنیتی این فروشگاه پیدا می‌کنند.

به گفته شرکت تحقیقاتی Upstream، میزان تراکنش‌های کلاهبرداری در پلتفرم‌های اندرویدی در سه ماهه اول سال جاری میلادی نسبت به مدت زمان مشابه در سال قبل، 55 درصد افزایش داشته و در تعداد گوشی‌هایی که در این بازه به بدافزارها آلوده شده‌اند، افزایش ناگهانی دیده می‌شود.

شرکت مذکور افزایش چشمگیر استفاده از برنامه‌های اندرویدی مخرب را به شیوع ویروس کرونا و قرنطینه ناشی از آن ربط داده است. به گفته کارشناسان این شرکت، افزایش برنامه‌های مخرب با اجرای قوانین قرنطینه اجباری رابطه مستقیم دارد و هکرها حبس شدن مردم در خانه‌ها را بهترین فرصت برای درآمدزایی دیده‌اند.

مخرب ترین برنامه اندرویدی در فصل اول سال جاری میلادی، «Snaptube» نام دارد که به کاربران اجازه دانلود ویدیو از شبکه‌های اجتماعی از جمله اینستاگرام، فیسبوک، توییتر و تیک تاک را داده و تاکنون بیش از 40 میلیون بار نصب شده است.


مرکز تخصصی آپا دانشگاه رازی