شماره نوزدهم - مرداد ۱۳۹۷

خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

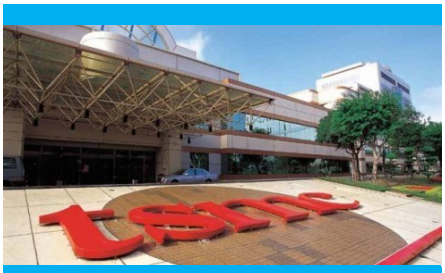
در این شماره خواهید خواند:

کاربران اینترنت اکسپلورر حداقل برای یک ماه در معرض آسیب پذیری روز صفر قرار گرفتند.

برای حداقل یک ماه، کاربران اینترنت اکسپلورر در معرض یک آسیب پذیری روز صفر قرار داشتند. با استفاده از این آسیب پذیری، مهاجم می‌تواند کنترل کامل کامپیوتر کاربران را به دست بگیرد. برای تبدیل شد به یک قربانی تنها کافیست که یک وب سایت آلوده را مشاهده نمایید. - صفحه ۲

خبرگان امنیت انگلیسی از شارژر USB-C اپل برای نشر بدافزار استفاده می‌کنند.

USB-C به عنوان یک رابط ارتباطی سریع و یک جک راحت برگشت پذیر مورد استفاده است که به دستگاه شما امکان شارژ شدن می دهد. این رابط یک روش اولیه برای حمله به دستگاه مورد نظر را به طرز ساده و ناخوشایندی فراهم می‌کند. - صفحه ۶



باج افزار ویندوزی که شرکت سازنده‌ی پردازنده‌های اپل آیفون را در تایوان هدف قرار داد.

از ماه ها پیش باج افزارها بلای جان مشاغل مختلفی همچون حمل و نقل، خدمات، بانک، بیمارستان و سایر شرکت‌ها در جهان شده‌اند. با رشد روز افزون این باج افزاها هرروزه اخبار بیشتری در خصوص آلوده شدن شرکت‌ها به گوش می‌رسد.
شرکت TSMC به دلیل حمله‌ی بدافزاری، مجبور به تعطیل کردن تمامی فعالیت‌هایش در هفته اول آگوست شد. این اتفاق برای بار اول برای این شرکت رخ داد که نیازمند توقف تمامی فعالیت‌هایش شد. - صفحه ۳

کشف ۱۷ آسیب پذیری در تنها ۴ دستگاه مربوط به شهر هوشمند

شهرهای هوشمند همچنان به حدی که مدیران آن فکر می کنند شفاف و ایده آل نیستند. طبق تحقیقاتی که به تازگی انجام شده است نقص های امنیتی بسیاری در وسایل مورد استفاده در شهرهای هوشمند وجود دارد. نکته ای که مهم است این است که فروشندگان وسایل مربوط به شهرهای هوشمند، حتی نکات ابتدایی امنیتی را رعایت نمی کنند. با بررسی چهار دستگاه ۱۷ آسیب پذیری کشف گردید که ۹ تا از این آسیب پذیری ها دارای درجه ی بحرانی می باشند. - صفحه ۴ و ۵

- **به گزارش Avast، هزاران خانه ی هوشمند در هند در معرض نشت اطلاعات قرار دارند.**

به گزارش دهلی نو، طی هشداری از سوی Avast، هزاران خانه هوشمند و کسب و کار در هندوستان در معرض خطر نشت اطلاعات به دلیل نقص در کانفیگ پروتکل های مورد استفاده در اتصالات خانه های هوشمند با hub ها هستند.- صفحه ۷

کاربران اینترنت اکسپلورر حداقل برای یک ماه در معرض آسیب پذیری روز صفر قرار گرفتند.

اینترنت اکسپلورر یکی از محبوب‌ترین مرورگرهای ارائه شده از سوی مایکروسافت است که دیگر جای خود را به مایکروسافت Edge داده است. اما این مرورگر محبوب هنوز طرفداران خاص خود را دارد که در سرتا سر دنیا همچنان از آن استفاده می‌کنند.

متاسفانه این مرورگر دارای نقص‌های امنیتی بسیاری می‌باشد که در سال‌ها کاربران را با مشکلات بزرگی روبه رو کرده است.

برای حداقل یک ماه، کاربران اینترنت اکسپلورر در معرض یک آسیب پذیری روز صفر قرار داشتند. با استفاده از این آسیب پذیری، مهاجم می‌تواند کنترل کامل کامپیوتر کاربران را به دست بگیرد. برای تبدیل شد به یک قربانی تنها کافیست که یک وب سایت آلوده را مشاهده نمایید.

دیروز، شرمت مایکروسافت یک وصله‌ی امنیتی برای این آسیب پذیری که حدود یک ماه پیش توسط یک آنتی ویروس کشف گردید، ارائه نمود. اکسپلویت مورد استفاده توسط مهاجم با متد مبهم سازی ایجاد گردیده بودکه در حملات روز صفر قبل نیز از آن استفاده می‌شد. این حمله موتور اجرای کدهای VBScript را مورد هدف قرار میدهد که توسط مایکروسافت در ماه می امسال وصله‌ی نرم افزاری آن ارائه گردید.

شباهت‌های زیادی بین اکسپلویت ماه می و جولای موجود است که طبق گمان های شرکت Trend Micro یک گروه ویا یک نویسنده پشت این ماجرا قرار دارند. شرکت های تولید کننده ی آنتی ویروس همچنین هشدار دادند که این آخرین حمله‌ی روز صفر نمی باشد.

شرکت Trend Microبرروی سایت خود اعلام نمود که: "این دومین اکسپلویت ایجاد شده با زبان VB است که در این سال ارائه شده است. دور از انتظار نیست که سایر آسیب پذیری های دیگری از موتور VB در آینده کشف گردد."

تولید کنندگان آنتی ویروس جزئیات بیشتری از ابعاد این نوع حمله را ارئه نکردند. اما با انتشار یک اسکرین شات از دامنه مورد استفاده ی مهاجمان برای بارگذاری اکسپلویت نشان می دهد که نام آن دامنه شامل کلمات "windows-updat" می باشد. بر اساس ادعای شرکتMicro Trend ویندوز اکسپلورر ۱۱ برروی ویندوز ۱۰ آپدیت Fall Creators دارای این آسیب پذیری نمی باشد زیرا VBScriptبه طور پیش فرض برروی این مرورگر غیر فعال است.

با این حال، مایکروسافت در بولتن امنیتی خود اعلام کرده است که اینترنت اکسپلورر در جدیدترین نسخه ویندوز ۱۰ واقعا آسیب پذیر است.

گردآورنده: محمد مرتضوی

باج افزار ویندوزی که شرکت سازنده‌ی پردازنده‌های اپل آیفون را در تایوان هدف قرار داد.

از ماه ها پیش باج افزارها بلای جان مشاغل مختلفی همچون حمل و نقل، خدمات، بانک، بیمارستان و سایر شرکت‌ها در جهان شده‌اند. با رشد روز افزون این باج افزاها هرروزه اخبار بیشتری در خصوص آلوده شدن شرکت‌ها به گوش می‌رسد.

حملات باج افزاری تا جایی رشد کرده‌اند که دیگر یک تهدید جدی برای صنایع حساب می‌شوند و به راحتی می‌توانند این صنایع را از پای در آورند.

با رشد رویکردهای امنیتی، همچنان باج افزارها به فعالیت خود ادامه می‌دهند. نمونه‌ی جدیدی که در این ماه روی داد در ادامه مورد بررسی قرار خواهد گرفت.

شرکت TSMC به دلیل حمله‌ی بدافزاری، مجبور به تعطیل کردن تمامی فعالیت‌هایش در هفته اول آگوست شد. این اتفاق برای بار اول برای این شرکت رخ داد که نیازمند توقف تمامی فعالیت‌هایش شد.

شرکت TSMC سازنده‌ی سری پردازنده‌های گجت‌های قدرتمندی همانند اپل آیفون است. TSMC همچنین برای شرکت NVIDIA، Qualcomm و AMD چیپ تولید می‌نماید.

چندین بخش ساخت TSMC توسط یک نوع از باج افزار Wansaware که برروی سیستم عامل ویندوز مایکروسافت عمل می‌کند در ۳ آگوست آلوده شدند. شدت آلوده شدن سیستم ها در هر بخش متفاوت بود.

در بیانه‌ای شرکت TSMC بیان نمود که مشکل به طور کامل شناسایی شده است و در حال رفع آن هستیم. در ۵ آگوست در ساعت ۱۴:۰۰ شرکت TSMC بیان نمود که در حدود ۸۰ درصد ابزارهایی که به باج افزار آلوده شده بودند با موفقیت بازیابی شدند.

تا کنون این شرکت توانسته است راه ورود باج افزار به شرکت را که از طریق یک شرکت ناشناس است تشخیص دهد. با این حال هنوز منبع آلودگی تشخیص داده نشده است.

معاون ارشد، سخنگو و مدیر مالی شرکت TSMC در نظر خود بیان کردند که : "این شیوع ویروس به دلیل سوء استفاده‌ای در طی فرآیند نصب نرم افزار برای یک ابزار جدید رخ داده است که باعث می شود ویروس پس از اتصال ابزار به شبکه کامپیوتری شرکت فعال گردد".

شرکت TSMC با این حال تاکید کرد که اطلاعات محرمانه و یکپارچگی داده ها در این حمله انتشار پیدا نکرده است و اعلان ها به تمام مشتریان ارسال شده است. Lora Ho از طریق مکالمه تلفنی در ۵ آگوست تأیید کرد که TSMC اقداماتی را برای بستن این شکاف امنیتی و اقدامات امنیتی بیشتری انجام داده است.

گردآورنده: محمد مرتضوی

کشف ۱۷ آسیب پذیری در تنها ۴ دستگاه مربوط به شهر هوشمند

شهرهای هوشمند همچنان به حدی که مدیران آن فکر می کنند شفاف و ایده آل نیستند. طبق تحقیقاتی که به تازگی انجام شده است نقص های امنیتی بسیاری در وسایل مورد استفاده در شهرهای هوشمند وجود دارد. نکته ای که مهم است این است که فروشندگان وسایل مربوط به شهرهای هوشمند، حتی نکات ابتدایی امنیتی را رعایت نمی کنند.

طی مطالعات اخیری که توسط X-Force Team شرکت IBM در کنفرانس Black Hat 2018 انتشار یافت، با بررسی چهار دستگاه ۱۷ آسیب پذیری کشف گردید که ۹ تا از این آسیب پذیری ها دارای درجه ی بحرانی می باشند. تمامی این دستگاه برای اتصال خودروها و سایر وسایل مورد استفاده قرار می گیرند. پیدایش این پروژه مربوط به یک خطای انسانی از سوی ساکنان هاوائی بود که اعتقاد داشتند جزایر آنان تحت حمله موشکی در ژانویه ۲۰۱۸ قرار داشته اند.

با توجه به این نکته، IBM تصمیم گرفت تا با بررسی سیستم، ببیند آیا محققان می توانند نقص هایی را پیدا کنند که منجر به حملات در "سطح فوق العاده" شوند. Crowley در خصوص نحوه شروع مطالعات بیان نمود:"ما به بررسی تکنیک های استفاده شده پرداختیم و سعی به هک آنان نمودیم. آسیب پذیری های بسیاری را به سرع یافتیم که ما را آشفته کرد". شرکت IBM دیوایس های i.LON 100/i.LON SmartServer و i.LON 600 از Echelon و V2I Hub v2.5.1 و V2I Hub v3.0 از Battelle را مورد بررسی قرار داد. معایب امنیتی شامل دستگاه هایی بود که در اینترنت دیده می شدند؛

در مورد دیگر، نرم افزاری متن باز با نام کاربری و رمز عبور Hard-Coded بود که یافتن اینگونه نام های کاربری و رمزهای عبور آسان است، نقص دیگری که یافت گردید در Shell آنان بود که به مهاجم دسترسی root اعطا می شد. برای نشان دادن یکی از این تهدیدات مربوط به حملات احتمالی، تیم Crowley یک فرآیند نمایشی برروی یکی از دستگاه-هایی که مورد مطالعه قرار دادند را از Meshlium IOT ایجاد نمودند. آنان از وسایل مانیتورینگ رایج همانند سنسور تشعشع استفاده نمودند و هر مشکلی را گزارش نمودند، که مخاطبان Black Hat را در معرض تابش قرار دادن، ایده جالبی نمی باشد، لذا تیم Crowley محصولات Meshlium را به یک سنسور آب متصل کرد و یک سیلندر را که سطح آب رودخانه را کنترل می کند را تحت اختیار خود درآورد. به علت نقص های shell در محصول Meshlium، Crowley قادر به هک کردن دستگاه و خواندن ورودی های غلط بود، در نتیجه آب بیش از حد آزاد شد و به جاده جعلی راه اندازی شد.

ادامه در صفحه‌ی بعد.

گردآورنده: محمد مرتضوی

کشف ۱۷ آسیب پذیری در تنها ۴ دستگاه مربوط به شهر هوشمند

(ادامه...)

Crowley بیان نمود: خبر خوب این است که فروشندگان، هنگامی که نقص ها گزارش شده بودند، در همه موارد به سرعت وصله های مربوطه را انتشار نمودند. اما مطالعات نشان داد که واضح است که تولیدکنندگان فکر و تأکید زیادی بر امنیت ندارند و آن را در اولویت کمتری قرار می دهند. Crowley بیان نمود که یکی از دلایلی که ما در این شرایط قرارگرفته ایم این است که تولید کنندگان تنها تمرکزشان برروی یافتن بازار فروش به عنوان اولین شرکت می باشد. علاوه بر آن، حتی انجام یک بررسی پایه ثابت می تواند جلوی آسیب پذیری-های بزرگی را بگیرد. در زیر لیستی از مشکلات یافت شده در دستگاه های شهر هوشمند قرار گرفته است:

Meshlium by Libelium - Wireless sensor networks

- (4) CRITICAL -- Pre-Authentication Shell Injection Flaw in Meshlium (four distinct instances)

i.LON 100/i.LON SmartServer and i.LON 600 by Echelon

- CRITICAL -- i.LON 100 default configuration allows authentication bypass - CVE -2018-10627
- CRITICAL -- i.LON 100 and i.LON 600 authentication bypass flaw - CVE-2018-8859
- HIGH -- i.LON 100 and i.LON 600 default credentials
- MEDIUM -- i.LON 100 and i.LON 600 unencrypted communications - CVE-2018-8855
- LOW -- i.LON 100 and i.LON 600 plaintext passwords - CVE-2018-8851

V2I (Vehicle-to-Infrastructure) Hub v2.5.1 by Battelle

- CRITICAL -- Hard-Coded Administrative Account - CVE-2018-1000625
- HIGH -- Sensitive Functionality Available Without Authentication - CVE-2018-1000624
- HIGH -- SQL Injection - CVE -2018-1000630 • HIGH -- Default API Key - CVE-2018-1000626
- HIGH -- API Key File Web Accessible - CVE-2018-1000627 • HIGH -- API Auth Bypass - CVE-2018-1000628
- MEDIUM -- Reflected XSS - CVE-2018-1000629

V2I Hub v3.0 by Battelle

- CRITICAL -- SQL Injection - CVE-2018-1000631

گردآورنده: محمد مرتضوی

خبرگان امنیت انگلیسی از شارژر USB-C اپل برای نشر بدافزار استفاده می‌کنند.

USB-C به عنوان یک رابط ارتباطی سریع و یک جک راحت برگشت پذیر مورد استفاده است که به دستگاه شما امکان شارژ شدن می دهد. قابلیت هایی نظیر Plug and Play و Self-Installation را نیز به خصوصیات آن اضافه نمایید، همچنین این رابط یک روش اولیه برای حمله به دستگاه مورد نظر را به طرز ساده و ناخوشایندی فراهم می کند.

رابط USB-C به دلیل قابلیت صرفه جویی در فضای فیزیکی به دلیل کاربرد چندگانه آن، اعم از رابط دیتا و شارژر در نوت بوک هایی نظیر MacBook Pro بسیار رایج می باشد. به گزارش BBC یک محقق امنیتی توانسته است از طریق رابط شارژر، یک بدافزار را برروی اپل اجرا نماید.

متخصص امور امنیتی USB با نام مستعار MG توانسته است شماری از بدافزارها را برروی گوشی های هوشمند از طریق USB نصب نماید. BBC با وی از طریق DEF CON آشنا گردید و در آخرین فعالیت هایش، وی در حال تلاش برای جذب دیگران در خصوص پروژه توسعه payload ها بود.

پروژه فعلی وی شامل تغییر یک شارژر اپل نسبت به مدل عادی آن و جایگزینی مدار قدرت داخلی با سخت افزار خود می باشد. تشخیص این نوع فریب بسیار مشکل است، چرا که شارژر همچنان به طور عادی عمل می کند و در حین شارژ کردن کامپیوتر شما (چه مک و چه پی سی)، قابلیت اجرا و نصب بدافزارهای مختلف را دارد. طبق گفته MG، این امر می تواند "نرم افزارهای مخرب، روت کیت ها و انواع مختلف آلودگی را که ممکن است مخرب باشد، به سیستم تزریق نماید."

این مفهوم در بین متخصصان تلفن همراه تعریف جدیدی را به خود تخصیص داده است و به نام "آب نوشیدن" مطرح می شود. با این حال، استفاده از USB-C در دستگاه های PC، ابعاد کاملا متفاوتی را شامل می شود. درست در لحظه‌ای که فکر میکنید می توانید به کافی شاپ بروید و از کسی بخواهید که لپ تاپ شما را شارژ کند.

گردآورنده: محمد مرتضوی

به گزارش Avast، هزاران خانه ی هوشمند در هند در معرض نشت اطلاعات قرار دارند.

به گزارش دهلی نو، طی هشداری از سوی Avast، هزاران خانه هوشمند و کسب و کار در هندوستان در معرض خطر نشت اطلاعات به دلیل نقص در کانفیگ پروتکل های مورد استفاده در اتصالات خانه های هوشمند با hub ها هستند.

محققان بیش از ۴۹،۰۰۰ سرویس پیام رسان پیام تله متری (MQTT) را در اینترنت کشف کردند که به دلیل تنظیمات غلط در دسترس هستند.

این مقدار شامل ۳۲۰۰۰ سرویس دهنده (که ۵۹۵ تا از آنان در هند قرار دارد) بدون پسورد می باشد که این سرورها را در خطر نشت اطلاعات قرار می دهد.

محقق امنیتی Avast، آقای Martin Hron بیان نمود که به طور وحشتناکی دسترسی و کنترل خانه های هوشمند مردم ساده می باشد. زیرا هنوز از دورانی که امنیت بحث اصلی دنیای تکنولوژی نبوده است پروتکل های ضعیفی وجود دارد. نیاز است تا مشتریان در خصوص اهمیت امنیت اتصال به وسایلی که بخش های مختلفی از خانه شان را کنترل می کند آگاه باشند و به درستی تنظیمات آن را اعمال کنند.

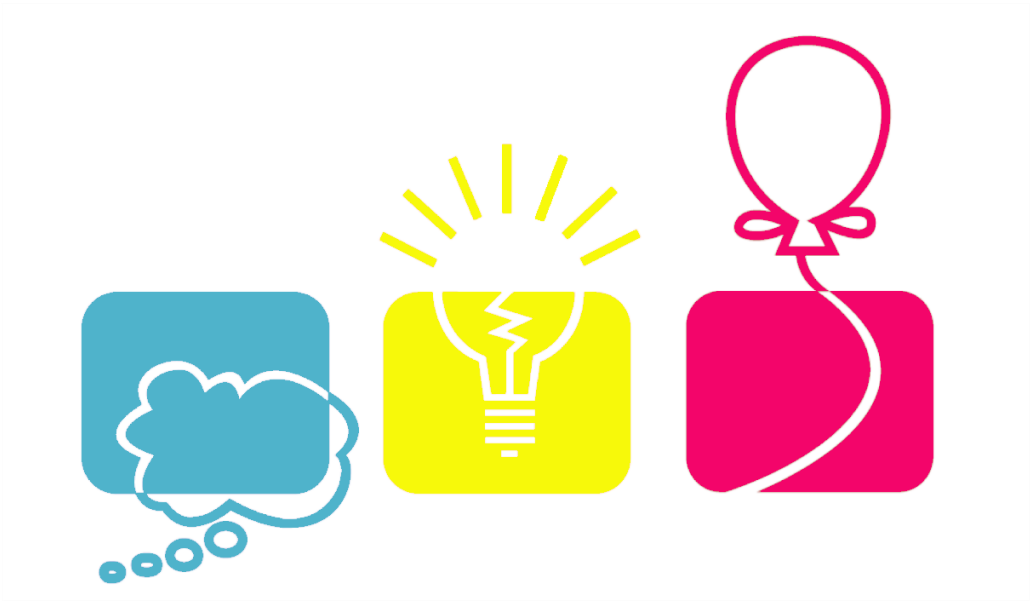
در هنگام راه اندازی پروتکل MQTT، کاربران یک سرویس دهنده را راه اندازی می کنند. در این موارد، عموما سرویس دهنده یک کامپیوتر شخصی ویا یک mini computer- همانند Raspberry Pi است که وسایل می توانند به آن متصل و ارتباط برقرار کنند.

خلافکاران سایبری می توانند دسترسی کامل به خانه ها پیدا کنند و در زمانی که صاحب خانه در خانه حضور دارد، سیستم صوتی و تصویری را آلوده نمایند و با استفاده از این سیستم ها بتوانند باز بودن ویا بسته بودن درب ها را بررسی نمایند.

در این حالت مهاجمان سایبری می توانند محل زندگی کاربر را ردگیری کنند و اطلاعات شخصی بسیار حساسی را استخراج نمایند.

گردآورنده: محمد مرتضوی

KHARAZMI CERT COORDINATOR CENTER



مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن نادری

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

http://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.