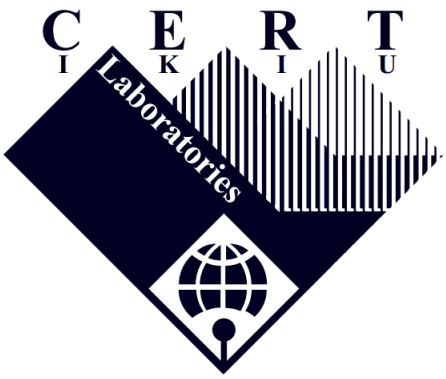


آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

هفته نامه تحلیلی رویدادهای امنیتی

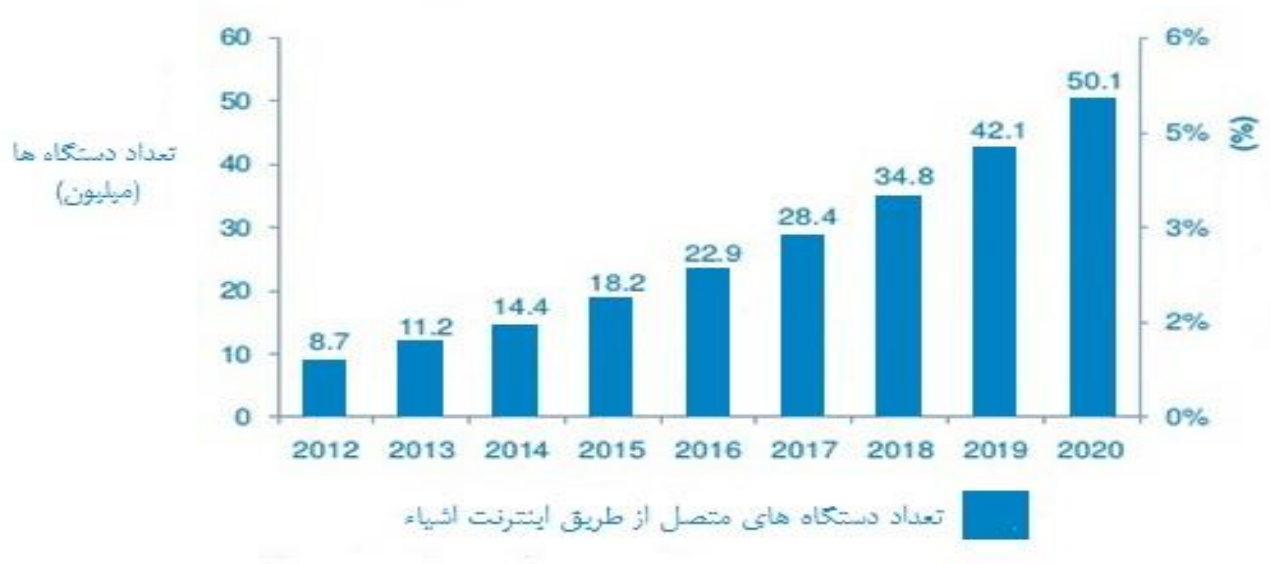
شنبه ششم مرداد ماه ۱۳۹۷

نسخه ۱,۰,۰

بنام خداوند بخشنده و مهربان

یادداشت سردبیر

بسیاری از فعالان حوزه فناوری اطلاعات از اینترنت اشیاء به عنوان یکی از فناوری‌های فراگیر در آینده بشر نام می‌برند. فناوری‌ای که با ترکیب اشیاء و اینترنت به دنبال تغییرات گسترده و کاربردی در زندگی انسان است. دیر یا زود پای ربات‌های هوشمند این فناوری به منازل ما ایرانی‌ها نیز باز خواهد شد (شکل ۱ میزان رشد دستگاه‌های بر اساس این فناوری را نشان می‌دهد). البته با گسترش اینترنت اشیاء تهدیدات امنیتی آن نیز گسترش خواهد یافت. تهدیداتی که می‌تواند از جنس آسیب‌رسانی فیزیکی به تجهیزات الکترونیکی نیز (از جمله قطع برق یک شهر) باشد. در همین راستا چند آسیب‌پذیری خطرناک در رابطه با یک نوع ماژول پر کاربرد در دستگاه‌های اینترنت اشیاء منتشر شده است. با توجه به ماهیت اینترنت اشیاء بهره‌گیری از آسیب‌پذیری‌های مذکور می‌تواند امکان جاسوسی غیرمجاز را نیز برای مهاجمان در شرایط و محیط‌های مختلف با توجه به نوع کاربرد به همراه داشته باشد.



شکل ۱ : پیش‌بینی تعداد دستگاه‌های اینترنت اشیاء در جهان تا سال ۲۰۲۰ (dontthinkjusteat.co)

خبر دیگر هفته گذشته به یک آسیب‌پذیری خطرناک در فناوری بلوتوث برمی‌گردد. فناوری‌ای نام آشنا که در بسیاری از دستگاه‌های الکترونیکی با نام‌های تجاری مختلف پیاده‌سازی شده است. با وجود این آسیب‌پذیری امکان شنود ارتباطات یا تزریق اطلاعات مخربی نظیر بدافزارها وجود دارد. البته برای این کار مهاجم باید در محدوده دریافت بلوتوث دستگاه‌های آسیب‌پذیر قرار بگیرد. آنچه در مورد این خبر اهمیت دارد وجود نام‌های تجاری معتبری از جمله اَپِل، اینتل[1] و کوالکام [2]در لیست محصولات آسیب‌پذیر است.

اما آخرین خبر هفته گذشته به برخی محصولات سیسکو ارتباط دارد. جایی که کلمات‌عبور ایستا منجر به نفوذ مهاجمان در سطح ریشه برخی نسخه‌های قدیمی ابزار پالسی‌سوئیت شده است. پالسی‌سوئیت یکی از ابزارهای سیسکو برای مدیریت شبکه در ترافیک و دسترسی‌های کاربران می‌باشد. چنین اشتباه امنیتی‌ای از شرکت سیسکو بسیار عجیب به نظر می‌رسد.

محمد پیشدار

[1]-Intel Corporation (stylized as intel) is an American multinational corporation and technology company headquartered in Santa Clara, California, in the Silicon Valley

[2]-Qualcomm is an American multinational semiconductor and telecommunications equipment company that designs and markets wireless telecommunications products and services

فهرست مطالب

خبر شماره ۱ تاریخ انتشار : ۹۷/۰۵/۰۲

کشف برخی آسیب‌پذیری‌ها در دستگاه‌های اینترنت اشیاء[1]

خلاصه

اخیرا محققان حوزه امنیت اطلاعات موفق به کشف آسیب‌پذیری‌های زیادی در دستگاه‌های اینترنت اشیاء شده‌اند. فناوری‌ای که با ایده پیوند اینترنت و اشیاء توانسته نظر بسیاری از سرمایه‌گذاران را نسبت به خود جلب نماید. آخرین نمونه این آسیب‌پذیری‌ها به یک جاروبرقی رباتیک خاص (ربات دیکی[2] ۳۶۰) مربوط می‌شود. نقصی که می‌تواند استراق سمع، سرقت تصاویر و اطلاعات شخصی را برای صاحبان آن به همراه داشته باشد. محققان استفاده از چیپستِ[3]های ارزان قیمت در دستگاه‌های اینترنت اشیاء را دلیل اصلی بسیاری از این آسیب‌پذیری‌ها دانسته‌اند.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=72

مرجع اصلی خبر:

InfoSecurity Website (https://www.infosecurity-magazine.com/news/vulnerable-iot-vacuums-dvrs-put/)

[1]-Internet of Things is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these things to connect and exchange data
[2]-Dongguan Diqee 360
[3]-Chipset

خبر شماره ۲ تاریخ انتشار : ۹۷/۰۵/۰۳

کشف آسیب‌پذیری خطرناک در محصولات سیسکو[1]

خلاصه

سیسکو در آخرین اطلاع رسانی خود خبر کشف ۲۵ آسیب‌پذیری مختلف را منتشر کرده است. چهار مورد از این آسیب‌پذیری‌های مذکور با درجه‌ی اهمیت بحرانی[2] می‌باشند [۱،۲]. هر چهار مورد به پالسی سوئیت یکی از معروف‌ترین ابزارهای شرکت سیسکو در حوزه شبکه مربوط می‌شود. پالسی سوئیت به عنوان یک محصول نرم‌افزاری در سه نسخه موبایل، وای‌فای[3] و بی‌اِن‌جی[4] در اختیار فراهم کنندگان خدمات اینترنت[5] قرار گرفته است. مدیران شبکه‌های بزرگ به وسیله این ابزار می‌توانند تمهیدات مدیریتی خود را بر پایه پهنای باند شبکه و میزان مصرف داده کاربران اعمال نمایند. علاوه بر این پالسی سوئیت قابلیت مشاهده‌ی کاربران و ترافیک مورد استفاده آن‌ها را نیز در شبکه فراهم می سازد. از بین چهار آسیب‌پذیری گفته شده همچنان یک مورد (سی‌وی‌اِی[6] ۲۰۱۸-۰۳۷۵) در برخی نسخه‌ی قدیمی محصولات سیسکو قابل بهره‌گیری[7] است. با بهره‌گیری از این نقص مهاجم می‌تواند به اجرای کدهای غیرمجاز در سیستم قربانی بپردازد.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=73

مرجع اصلی خبر:

securityweek(https://www.securityweek.com/cisco-finds-serious-flaws-policy-suite-sd-wan-products)

[1] Cisco (Cisco Systems, Inc. is an American multinational technology conglomerate headquartered in San Jose, California, in the center of Silicon Valley)
[2] critical
[3] WIFI
[4] Broadband Network Gateway
[5] Internet Service Provider
[6] CVE
[7] -Exploit

خبر شماره ۳ تاریخ انتشار : ۹۷/۰۵/۰۴

کشف آسیب‌پذیری خطرناک در فناوری بلوتوث[1]

خلاصه

اخیرا محققان حوزه امنیت اطلاعات مدعی وجود یک آسیب‌پذیری خطرناک در برخی پیاده‌سازی‌های بلوتوث شده‌اند. آسیب‌پذیری‌ای که تنها مربوط به دستگاه‌های نام‌های تجاری گمنام نبوده و حتی محصولات شرکت‌های بزرگ را نیز شامل می‌گردد. نام‌هایی از جمله اَپِل، کوالکام[2]، اینتِل[3]، اَندروید و حتی لینوکس نیز در زمره قربانیان این آسیب‌پذیری قرار می گیرد. نقصی که به مهاجم غیرمجاز توانایی شنود، نظارت و یا حتی دستکاری اطلاعات انتقالی را در یک ارتباط بلوتوث خواهد داد. البته برای این کار مهاجم باید در محدوده سیگنال (حدود چند متر) بلوتوث دستگاه‌های آسیب‌پذیر حضور داشته باشد.

برای مشاهده متن کامل خبر می‌توانید به آدرس زیر مراجعه نمایید.

https://cert.ikiu.ac.ir/news-view.php?nid=74

مرجع اصلی خبر:

Carnegie University Cert (https://www.kb.cert.org/vuls/id/304725)

[1]-Bluetooth

[2]-Qualcomm is an American multinational semiconductor and telecommunications equipment company that designs and markets wireless telecommunications products and services

[3]-Intel Corporation (stylized as intel) is an American multinational corporation and technology company headquartered in Santa Clara, California, in the Silicon Valley