شماره هفتم – نیمه اول بهمن ماه ۱۳۹۶

خبرنامه "آپا" دانشگاه محقق اردبیلی

در این شماره می‌خوانیم:

- ✓ جایگاه حملات سایبری در بین دیگر تهدیدهای جهان در سال ۲۰۱۸
- ✓ کشف بدافزار غیرقابل شناسایی با قابلیت اجرا بر روی تمامی سیستم‌عامل‌ها
- ✓ کشف آسیب¬پذیری بحرانی در برنامه¬های کاربردی ایجاد شده با Electron
- ✓ مشکل احراز هویت در Libcurl
- ✓ آمار افزونه‌ها و قالب‌های آسیب‌پذیر وردپرس
- ✓ آلوده شدن بیش از ۴,۵ میلیون کاربر به آگهی‌افزار توسط بازی‌های مخرب اندرویدی
- ✓ هک کامپیوتر کاربران با بهره‌برداری از نقص برنامه Transmission BitTorrent
- ✓ فریب کاربران به دانلود باج‌افزار با استفاده از ارزرمزی جعلی
- ✓ نمایش موقعیت پایگاه‌های نظامی محرمانه با استفاده از نقشه حرارتی منتشر شده توسط ردیاب تناسب اندام
- ✓ افزایش تولید باج‌افزار در سال ۲۰۱۷ نسبت به سال‌های دیگر
- ✓ وصله شدن آسیب‌پذیری‌های بحرانی شبکه‌ی مجازی خصوصی (VPN) سیسکو
- ✓ وجود یک آسیب‌پذیری بحرانی در کارگزار وب مورد استفاده در بیش از ۱۰۰ محصول سامانه‌ی کنترل صنعتی
- ✓ مجهز شدن پردازنده‌های AMD به محافظت دربرابر بهره‌برداری‌های مشابه Spectre

045 31505718
cert@uma.ac.ir
اردبیل - خیابان دانشگاه - دانشگاه محقق اردبیلی

جایگاه حملات سایبری در بین دیگر تهدیدهای جهان در سال ۲۰۱۸

مؤسسه تحقیقاتی WEF گزارشی در مورد تهدیدها و ریسک‌های جهانی ارائه داده است. در این گزارش، فهرستی از مشکلات و خطرهای احتمالی و بالقوه‌ای که در جهان ممکن است رخ دهد و مردم کشورهای مختلفی را با دشواری‌های بسیاری روبرو کند، بیان شده است. دیدگاه ۱۰۰۰ کارشناس جهانی برای جمع‌آوری این ریسک‌ها و خطرهای احتمالی قابل توجه در سال ۲۰۱۸، مورد بررسی قرار گرفته است.

این خطرات در حوزه‌های تکنولوژی، اقتصادی، اجتماعی، سیاسی و زیست محیطی قرار دارند. بر اساس این گزارش، جرایم سایبری و سرقت اطلاعات افراد و سازمان‌ها توسط مجرمان سایبری و بدافزارها جایگاه نخست را در بین خطرناک‌ترین تهدیدات جهان به خود اختصاص داده است. پس از حملات سایبری، مشکلات زیست محیطی مانند خشکسالی و آلودگی هوا، مهاجرت‌های اجباری گسترده و فجایع طبیعی همچون زمین لرزه و تجارت‌های غیرقانونی و نامشروع همچون قاچاق اسلحه و دارو، به ترتیب در جایگاه‌های دوم تا پنجم قرار گرفته‌اند.

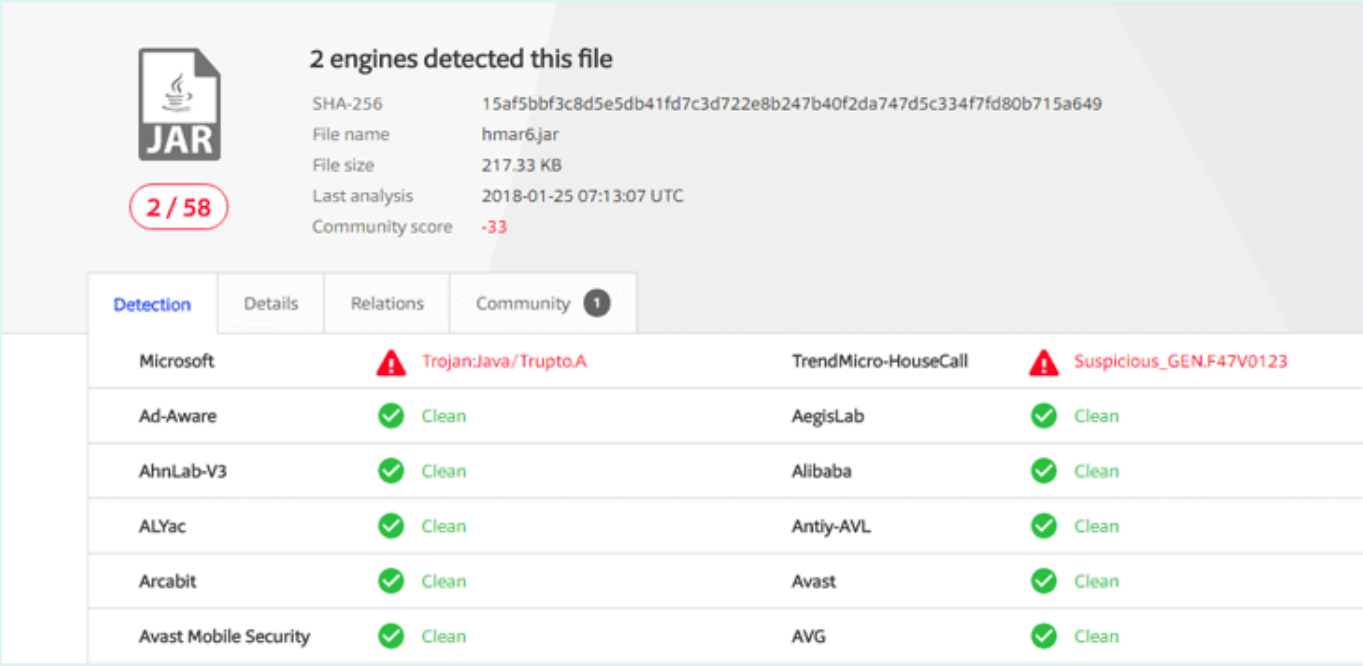
پنج رویداد مهمی که به احتمال زیاد در سال ۲۰۱۸ رخ خواهد داد و پیش‌تر بیان شد، کمی متفاوت از لیست رویدادهایی است که بزرگترین تأثیر جهانی را دارند. رویدادهای تأثیرگذار جهانی، سلاح‌های کشتار جمعی، حوادث شدید آب و هوایی، بلایای طبیعی، تغییرات اقلیمی و بحران آب می‌باشند. از ۱۰۰۰ کارشناس جهانی که مورد پرسش قرار گرفتند، ۵۹ درصد معتقد بودند که خطرهای جهانی در سال ۲۰۱۸ تشدید می‌شوند، اما هفت درصد معتقدند میزان خطرها در سطح جهانی کاهش خواهد یافت. در سال‌های قبل از سال ۲۰۰۸ هیچ نگرانی در مورد تهدیدها و جرایم سایبری وجود نداشته است اما با توجه به رشد و توسعه تکنولوژی و دسترسی مردم به اطلاعات مهم، این حملات یکی از مهم‌ترین تهدیدهای جهانی به شمار می‌رود. نتایج و یافته‌های تحقیقات و پژوهش‌های انجام شده نشان می‌دهد که میزان حملات سایبری در سال جاری به اوج خود خواهد رسید؛ بنابراین تمامی شرکت‌ها در سراسر جهان وظیفه دارند که اقدامات لازم را برای مقابله با حملات انجام دهند تا در برابر حملات و خسارات جبران ناپذیر هکرها، آسیب‌پذیری کمتری داشته باشند و میزان امنیت اطلاعات خود و مشتریان را تا حدودی تضمین کنند. بر اساس گزارش‌های منتشر شده، بدافزارها، باج‌افزارها و حملات DDOS از جمله تهدیدهای امنیتی بودند که از سال ۲۰۱۶ تا به حال کاربران فضای مجازی را در معرض خطر حملات سایبری قرار داده و باعث افشای اطلاعات شخصی و محرمانه آن‌ها شده‌اند. طبق آمار، حملات سایبری در سال ۲۰۱۷ نیز به اوج خود رسیده بود و گزارش‌ها حاکی از آن است که در سال‌های آتی اوضاع نابسامان‌تر می‌شود. در سال گذشته باج‌افزارها، بدافزارها و ویروس‌های رایانه‌ای بسیاری در سراسر جهان، انواع اطلاعات محرمانه، خصوصی و مالی میلیون‌ها نفر را به سرقت بردند و میلیاردها دلار به شرکت‌های مربوطه و دولت‌ها خسارت وارد کرده‌اند. برای مثال حمله سایبری باج‌افزار WannaCry یکی از مهلک‌ترین حملاتی است که در طول چندین سال اخیر صورت گرفته است.

منبع: scmagazineuk ترجمه: سحر علیزاده

کشف بدافزار غیرقابل شناسایی با قابلیت اجرا بر روی تمامی سیستم‌عامل‌ها

طیف وسیعی از مجرمان سایبری اکنون از یک تروجان جدید جاسوسی غیر قابل شناسایی استفاده می‌کنند که قادر است بر روی سیستم‌عامل‌های مختلف اجرا شود. این بدافزار را که محققان CrossRAT نامیده‌اند، یک تروجان دسترسی از راه دور Cross-Platform است که می‌تواند بر روی هر ۴ سیستم‌عامل دسکتاپی محبوب ویندوز، لینوکس، Mac و Solaris را اجرا شود.

این بدافزار مهاجمان را قادر می‌سازد تا سیستم‌فایل را دستکاری کنند، از صفحه مانیتور عکس بگیرند، فایل‌های اجرایی دلخواهی را اجرا کنند و در سیستم‌های آلوده



پایداری لازم برای خود بدست آورند. محققان بر این باورند که این بدافزار توسط گروه Caracal Dark توسعه داده شده است. هکرهای Dark Caracal به هیچ اکسپلویت روزصفر برای توزیع بدافزارشان متکی نشده‌اند و به جای آن از روش‌های مهندسی اجتماعی مانند استفاده از پست‌ها و گروه‌های فیسبوک و پیام‌های WhatsApp استفاده می‌کنند و کاربران را به بازدید از وب‌سایت‌های جعلی کنترل شده توسط هکرها و دانلود برنامه‌های مخرب تشویق می‌کنند. CrossRAT با زبان برنامه‌نویسی جاوا نوشته شده است و با اینکه باعث می‌شود بتواند بر روی چندین سیستم‌عامل کار کند، اما مهندسی معکوس و دیکامپایل کردن آن آسان می‌گردد. در زمان انتشار گزارش مربوط به این بدافزار، بر اساس نتیجه اسکن این بدافزار روی سامانه virustotal، تنها ۲ آنتی‌ویروس از ۵۸ آنتی‌ویروس موفق به شناسایی آن را شدند. در شکل بالای صفحه نتیجه بررسی این فایل (با نام hmar6.jar) روی سامانه virustotal آورده شده است.

زمانی که این بدافزار بر روی سیستم هدف اجرا می‌شود، ابتدا نوع سیستم‌عامل را بررسی می‌کند و بر اساس نوع سیستم‌عامل، خود را راه‌اندازی می‌کند. علاوه بر این، تلاش می‌کند تا اطلاعاتی را در مورد سیستم آلوده به‌دست آورد. این اطلاعات شامل نسخه سیستم‌عامل نصب شده، ساخت Kernel و معماری می‌باشد. این بدافزار بر روی سیستم‌های لینوکسی تلاش می‌کند تا فایل‌های systemd را برای تعیین توزیع آن (Arch Linux، CentOS، Debian، Kali، Fedora و Mint) جستجو کند؛ سپس مکانیزم‌های پایداری خود را به‌صورت اختصاصی برای هر سیستم‌عامل اجرا می‌کند. این کار به این منظور انجام می‌شود که بدافزار بتواند به‌صورت خودکار در هر زمان که سیستم دوباره شروع به کار شد، اجرا شود و خود را در سرور کنترل و فرمان (C&C) ثبت کند تا مهاجمان از راه دور بتوانند دستوراتی را ارسال کرده و اطلاعات مورد نظرشان را استخراج کنند. طبق گزارش‌ها این بدافزار به "flexberry.com"و بر روی پورت ۲۲۲۳ متصل می‌شود. این بدافزار با برخی قابلیت‌های پایه‌ای نظارت طراحی شده است که هرکدام از این قابلیت‌ها فقط زمانی که دستورهای مخصوص ازپیش‌تعریف‌شده را از سرور کنترل و فرمان (C&C) دریافت کنند، اجرا می‌شوند.

بررسی‌های محققان، نشان می‌دهند که بدافزار از یک کتابخانه متن‌باز جاوا به نام "jnativehook" استفاده می‌کند. این کتابخانه برای گوش دادن به رویدادهای ماوس و صفحه‌کلید استفاده می‌شود، اما این بدافزار هیچ دستور از پیش‌تعریف‌شده‌ای برای فعال‌سازی این Keylogger ندارد؛ بنابراین می‌توان نتیجه گرفت که از

این قابلیت برای نفوذ استفاده نشده است. از آن‌جا که CrossRAT هر سیستم‌عامل را به‌صورت اختصاصی مورد هدف قرار می‌دهد، تشخیص آن بستگی به نوع سیستم‌عاملی دارد که شما از آن استفاده می‌کنید.

- برای ویندوز:

کلید رجیستری زیر را بررسی کنید:
"HKCU\Software\Microsoft\Windows\CurrentVersion\Run\"
در صورتی که ویندوز شما آلوده شده باشد، حاوی یک دستور خواهد بود که شامل java، jar- و mediamgrs.jar می‌باشد.

- برای سیستم‌عامل Mac:

فایل mediamgrs.jar در مسیر ~/Library جستجو کنید. همچنین در مسیرهای ~/Library/LaunchAgents یا /Library/LaunchAgents، عامل اجرا این بدافزار با نام mediamgrs.plist را جستجو کنید.

- برای لینوکس:

فایل mediamgrs.jar را در /usr/var جستجو کنید. همچنین در مسیر ~/.config/autostart فایل "autostart" را که احتمالا با نام mediamgrs.desktop قرار دارد، پیدا کنید.

جهت جلوگیری از فعالیت این بدافزاری، توصیه می‌شود که کاربران نرم‌افزار تشخیص تهدیدات رفتارمحور نصب کنند.

منبع: thehackernews گردآوری: معصومه خیری

کشف آسیب‌پذیری بحرانی در برنامه‌های کاربردی ایجاد شده با Electron

چارچوب Electron تحولی در زمینه تولید نرم‌افزارهای دسکتاپی می‌باشد. چارچوب Electron، فناوری متن‌باز جدیدی برای ساخت نرم‌افزارهای دسکتاپ چندسکویی (Cross-platform Native Desktop Applications) می‌باشد. این چارچوب با استفاده از فناوری‌های وب HTML، CSS و جاوااسکریپت و همچنین بهره‌گیری از موتور مرورگر Chromium می‌تواند نرم‌افزار دلخواه شما را در لینوکس، MacOS و ویندوز ایجاد و اجرا کند. این روش باعث می‌شود توسعه‌دهندگان هنگام استفاده از این چارچوب، نیازی به آشنایی با زبان برنامه‌نویسی استفاده شده در هر سیستم‌عامل جهت تولید نرم‌افزار نداشته باشند. به کمک این چارچوب بسیاری از برنامه‌های کاربردی مطرح تحت ویندوز مانند Slack، Skype، Signal، Atom، VScode و WordPressتولید شده‌اند.

به تازگی آسیب‌پذیری بسیار خطرناک در این چارچوب کشف شده است. این آسیب‌پذیری دارای شماره شناسه CVE-2018-1000006 در پایگاه‌داده آسیب‌پذیری می‌باشد و تنها برنامه‌های کاربردی تحت ویندوزی را که از اجراکننده پیش‌فرض (Default Handler) جهت ثبت پروتکل‌هایی مانند tg:// که تلگرام استفاده می‌کند، تحت تاثیر قرار می‌دهد. زمانیکه یک برنامه به عنوان اجراکننده پیش‌فرض برای پروتکلی ثبت می‌شود، این قابلیت به برنامه اضافه می‌شود که بتوان برنامه را با کلیک بر روی لینک (که با نام پروتکل ثبت شده شروع می‌شود) اجرا کرد. به این ترتیب هرگاه کاربر نشانی وب متناسب با برنامه را فراخوانی کند برنامه فعال خواهد شد.

تیم Electron در طی خبری اعلام کرد که از هر روشی برای ثبت برنامه بعنوان اجراکننده پیش‌فرض استفاده شود، برنامه تحت تاثیر این آسیب‌پذیری قرار می‌گیرند. همچنین این شرکت تاکید کرد که برنامه‌های کاربردی طراحی شده برای لینوکس، MacOS و آن دسته از برنامه‌های تحت ویندوز که به عنوان اجراکننده پیش‌فرض برای پروتکل‌ها ثبت نشده‌اند، آسیب‌پذیر نیستند. هم اکنون نسخه‌های جدید 1.8.2-beta.4، 1.6.16 و1.7.11 برای رفع این آسیب‌پذیری منتشر شده است.

تیم Electron از توسعه‌دهندگان خواسته است که اگر به هر دلیلی نمی‌توانند نسخه چارچوب Electron را ارتقا ببخشند، از علامت "–" بعنوان آخرین آرگومان ارسالی در فراخوانی تابع app.setAsDefaultProtocolClient() استفاده کنند تا مانع از پردازش آرگومان‌های دیگر در موتور مرورگر Chromium شوند. از آنجایی که کاربران

استفاده‌کننده از برنامه کاربردی آسیب‌پذیر، راهکاری جهت جلوگیری از مورد سوء استفاده قرار گرفتن توسط این تهدید ندارند، توسعه‌دهندگانی که از Electron JS استفاده می‌کنند باید برنامه‌های خود را جهت رفع این آسیب‌پذیری ارتقا دهند. جزئیات بیشتری از این آسیب-پذیری وجود ندارد. همچنین به دلایل امنیتی نام برنامه-های کاربردی آسیب‌پذیر فعلا منتشر نشده است.

منبع: thehackernews مترجم: سمیرا سیفی

مشکل احراز هویت در Libcurl

اگر از ابزار و کتابخانه خط فرمان Libcurl برای انتقال‌داده با پروتکل‌های مختلف و بر اساس URL استفاده می‌کنید، باید آن را وصله کنید. محققان می‌گویند که این کتابخانه به دلیل استفاده از روش نامناسب در مدیریت سرآیند دلخواه، اطلاعات احراز هویت را افشا می‌کند.

Curl این امکان را برای کاربران خود فراهم کرده است تا مقادیر سرآیند (Header) ارسالی را بازنویسی کنند یا مقادیر جدیدی را به سرآیند درخواست HTTP ارسالی اضافه کنند و سرآیندهای دلخواه خود را تولید نمایند. Libcurl زمانی که باید سرآیندهای دلخواهی را در درخواست‌های HTTP ارسال کند، این مجموعه سرآیندها را به URL که در درخواست‌ها مشخص شده، ارسال می‌کند. در صورتی که در پاسخ درخواست ارسال شده، کدهای تغییر مسیر (301,302,303) را دریافت کند، در-خواست‌ها به مسیر جدیدی که از سمت سرور مشخص شده است، هدایت می‌شوند. به همراه این تغییر مسیر، ممکن است اطلاعات احراز هویت نیز ارسال شود. بنابراین Libcurl در زمان تغییر مسیر، اطلاعات احراز هویت یا داده‌های مهمی (داده‌هایی که می‌توانند برای جعل درخواست Libcurl استفاده شوند) را نشت می‌دهد؛ و برنامه‌هایی که اطلاعات احراز هویت آن‌ها از طریق این سرآیندهای دلخواه (برای مثال Authorization) انتقال می‌یابند، آسیب‌پذیر هستند. آسیب‌پذیری مذکور که دارای شناسه CVE-2018-1000007 در پایگاه‌داده آسیب‌پذیری می‌باشد از نسخه 6.0 این کتابخانه وجود داشته است. این نسخه در سال ۱۹۹۹ منتشر شده است، لذا این آسیب‌پذیری در ۱۸ سال اخیر تمامی برنامه‌های استفاده کننده از این کتابخانه را تحت تاثیر قرار داده است. البته محققان بر این عقیده هستند که این آسیب‌پذیری از زمان اولین انتشار این ابزار (سال ۱۹۹۷) نیز وجود داشته است.

کاربران برای رفع این مشکل باید Curl خود را به نسخه 7.58.0 بروزرسانی کنند. از آنجایی که با این بروزرسانی رفتار نرم‌افزار تغییر خواهد کرد، اگر کاربران نیازمند ارسال سرآیند به سایت دیگری هستند باید به ابزار اجازه تغییر مسیر درخواست را با ارسال پارامتر location-trusted-- که یک عبارت کنترلی است را بدهند.

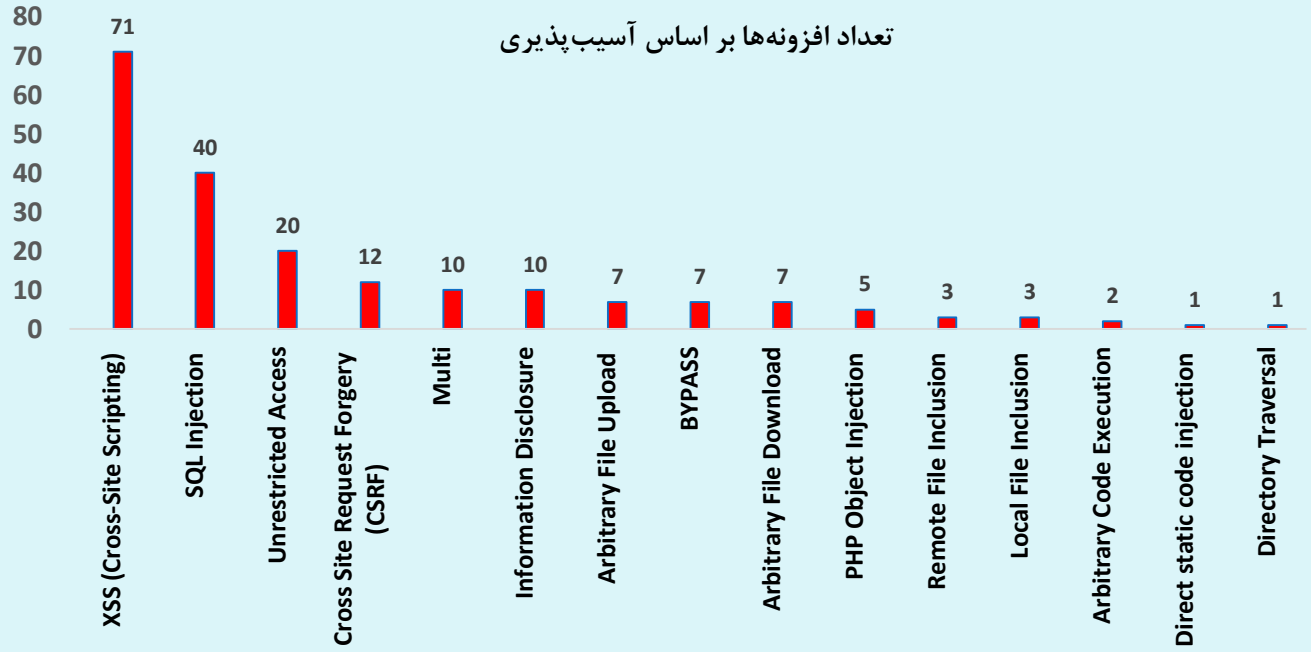
منبع: theregister مترجم: سمیرا سیفی

آمار افزونه‌ها و قالب‌های آسیب‌پذیر وردپرس

در این خبر مروری خواهیم داشت بر اطلاعات آماری آسیب‌پذیری قالب‌ها و افزونه‌های وردپرس در سال ۲۰۱۷، که طی بررسی و نظارت بر پایگاه‌داده آسیب‌پذیری‌های وردپرس کشف شده است. در سال ۲۰۱۷، ۲۲۱ آسیب-پذیری به این پایگاه‌داده اضافه شده است و تعداد کل آسیب‌پذیری‌های شناسایی شده نسبت به سال قبل حدود ۶۹٪ کاهش دارد. این آسیب‌پذیری‌ها بیش از ۱۷,۱۰۱,۳۰۰ سایت را در معرض خطر قرار می‌دهند.

کشف آسیب‌پذیری Cross-Site Scripting (XSS) در سال ۲۰۱۷ همچنان در صدر آسیب‌پذیری‌ها قرار دارد. تعداد افزونه‌ها و قالب‌های کشف شده که دارای آسیب-پذیری XSS هستند رو به افزایش می‌باشد و دلیل اصلی این افزایش بی‌توجهی توسعه‌دهندگان به اعتبارسنجی داده‌های خروجی می‌باشد. در سال ۲۰۱۷ همچنین تعداد آسیب‌پذیری‌های SQL Injection به صورت قابل ملاحظه‌ای افزایش یافته است.

حقایق جالب دیگری در مورد وردپرس وجود دارد که ازجمله می‌توان به انتشار ۸ بروزرسانی در سال ۲۰۱۷،



شناسایی اولین آسیب‌پذیری در تاریخ ۲۰ فوریه سال ۲۰۰۵ و وجود ۳,۳۲۱ آسیب‌پذیری در پایگاه‌داده آسیب-پذیری ThreatPress اشاره کرد.

نگاهی اجمالی به آسیب‌پذیری‌های وردپرس

- ۲۱۲ افزونه آسیب‌پذیر
- ۵ قالب آسیب‌پذیر
- ۱۵۳ افزونه تحت تاثیر آسیب‌پذیری‌ها موجود در مخزن WordPress.org
- ۲۴ افزونه تحت تاثیر آسیب‌پذیری‌ها موجود در مخازنی غیر از WordPress.org

۵ قالب معروف تحت تاثیر آسیب‌پذیری‌ها

نام افزونه	تعداد	نوع آسیب‌پذیری
Yoast SEO	۵,۰۰۰,۰۰۰	XSS
WooCommerce	۳,۰۰۰,۰۰۰	XSS
Smush Image Compression and Optimization	۱,۰۰۰,۰۰۰	Directory Traversal
Duplicator	۱,۰۰۰,۰۰۰	XSS
Loginizer	۶۰۰,۰۰۰	SQL Injection

منبع: securityaffairs مترجم: سمیرا سیفی

آلوده شدن بیش از ۴,۵ میلیون کاربر به آگهی‌افزار توسط بازی‌های مخرب اندرویدی

کامپونت‌های موجود در یک برنامه اندروید که قابلیت گفتگو بین کاربران را فراهم می‌کرد در پس‌زمینه تلفن همراه بطور مخفیانه سایت‌هایی را باز کرده و بر روی تبلیغات کلیک می‌کرده‌است.

براساس گزارش‌های انتشار یافته، این کامپونت‌های مخرب، در قسمتی از کیت توسعه نرم‌افزار (SDK) بوده که به یک شرکت چینی با نام YaYaYun ارائه شده است. توسعه‌دهندگان برنامه اندروید از SDK برای اضافه کردن یک بخش گفتگو بعنوان یک ویژگی به بازی که در حال توسعه آن بودند، استفاده کرده‌اند. وجود این ویژگی توسعه‌دهندگان را ترغیب کرد تا بدلیل اینکه بازی سریع آماده گردد به جنبه‌های دیگر بازی پرداخته و به بخش گفتگو توجهی نکنند.

استفاده از SDK برای توزیع امکانات مختلف نرم‌افزارها در سرورهای راه دور جهت فراهم کردن امکان کنترل از راه دور برای شرکت ارائه‌دهنده SDK که در برنامه‌های شرکت YaYaYun استفاده شده‌اند، خطرناک می‌باشد. با توجه به گفته‌های شرکت آنتی‌ویروس روسی Dr.Web در مورد بازی‌های اندرویدی که توسعه‌دهندگان آن‌ها از

SDK مربوط به YaYaYun استفاده کرده‌اند اعتماد به آن بازی‌ها از بین می‌رود.

محققان شرکت امنیتی تلفن همراه اعلام کرده‌اند که برنامه‌هایی که با استفاده از این SDK توسعه داده شده‌اند را در فروشگاه‌های معتبری همچون Google Play مشاهده کرده‌اند. بر اساس اظهارات Dr.Web هنگام دانلود این برنامه‌ها، اجزای مخرب در داخل آن‌ها مخفی شده و به سیستم قربانی انتقال داده می‌شوند.

Ya Ya Yun SDK این تصاویر را دانلود کرده و اجزای مخربی را که در داخل آن‌ها مخفی شده‌اند را بازکرده و از آن‌ها در دستگاه کاربران استفاده می‌کند. در حال حاضر، اجزای دانلود شده فقط آن URL را که درون یک مرورگر مخفی شده است، باز کرده و بر روی تبلیغات به نفع کلاه-برداران کلیک می‌کنند؛ اما کارشناسان می‌گویند که این امر می‌تواند به‌سادگی به دیگر اقدامات مخرب تبدیل گردد.

کارشناسان شرکت Dr.Web در گزارشی که هفته پیش ارائه داده‌اند، اعلام کردند که: "نویسندگان ویروس قادر به ایجاد ماژول‌های تروجان دیگری نیز هستند که دیگر فعالیت‌های مخرب را انجام می‌دهند. ایجاد یک صفحه Phishing برای سرقت اطلاعات ورود، نمایش تبلیغات و همچنین دانلود و نصب برنامه‌ها بصورت مخفیانه از جمله آن‌ها می‌باشد."

همچنین بیش از ۴,۵ میلیون کاربر توسط تروجان Android.RemoteCode.127 آسیب دیده‌اند. محققان این رفتار مخرب را در ۲۷ بازی اندرویدی که از طریق Play Store در دسترس بوده، یافته‌اند که در بیش از ۴,۵ میلیون دستگاه نصب شده است. کارشناسان می‌گویند که این برنامه‌های مخرب را به گوگل اعلام کرده‌اند.

چند روز بعد از اینکه گزارش Dr.web منتشر شد شرکت Bleeping رفتار بسیاری از برنامه‌هایی را که در گزارش آمده بود را مورد بررسی قرار داد که اکثر آن‌ها همچنان در Play Store قرار دارند.

در موارد مشابه که قبلا اتفاق افتاده بود شرکت گوگل اغلب برنامه‌هایی که دارای SDK مخرب بوده، غیرفعال می‌کرد تا توسعه دهندگان، اجزای مخرب را از روی برنامه خود حذف کنند. درحالی‌که بیشتر این برنامه‌ها همچنان در دسترس هستند ولی ممکن است اهداف و رفتار مخربانه مانند نداشته باشند. از آنجایی‌که نمی‌توان درباره این ویژگی در این برنامه‌ها برای اجرای مقاصد مخرب اظهار نظر کرد؛ بنابراین عدم استفاده از برنامه‌های زیر توصیه می‌شود.

Gumballs & Dungeons : Roguelike RPG Dungeon crawler	Warship Rising - 10 vs 10 Real-Time Esport Battle
Thủy Chiến - 12 Vs 12	King of Warship: National Hero
King of Warship:Sail and Shoot	Never Find Me - 8v8 real-time casual game
خاتم التنين - Dragon Ring (For Egypt)	Kıyamet Kombat Arena
Dance Together	Love Dance
Star Legends	Fleet Glory
Sword and Magic	perang pahlawan
Royal flush	Soul Awakening
Sword and Magic	Clash of Civilizations
Era of Arcania	Hero Mission

منبع: Bleepingcomputer مترجم : ابوالفضل علیقلی‌وند

هک کامپیوتر کاربران با بهره‌برداری از نقص برنامه Transmission BitTorrent

در برنامه Transmission BitTorrent که به‌طور گسترده توسط کاربران مورد استفاده قرار می‌گیرد، یک آسیب‌پذیری حیاتی کشف شده است. مهاجمان با استفاده از این آسیب‌پذیری می‌توانند یک کد مخرب را از راه دور بر روی کامپیوترهای کاربران BitTorrent اجرا کرده و کنترل کامپیوتر آنان را در اختیار بگیرند.

برنامه Transmission اجازه می‌دهد تا کاربران به سرعت فایل‌ها را از چندین peer در اینترنت دانلود و یا فایل‌های خود را بارگذاری کنند.

آسیب‌پذیری مذکور (با شناسه CVE-2018-5702) توسط تیم گزارش‌گر آسیب‌پذیری گوگل یعنی Project Zero کشف شد. یکی از اعضای این تیم به نام Tavis Ormandy پس از ۴۰ روز از گزارش اولیه، ادعای وجود این آسیب‌پذیری را اثبات و منتشر کرد.

تیم Project Zero معمولا آسیب‌پذیری‌ها را ۹۰ روز بعد از ارائه گزارش اولیه به شرکت یا تیم توسعه‌دهنده سرویس موردنظر به صورت عمومی منتشر می‌کند تا شرکت مربوطه زمان کافی برای حل مشکل داشته باشد و بتواند قبل از همگانی شدن آسیب‌پذیری یک وصله مناسبی ارائه کند.

بااین‌حال، در این مورد، محققان Project Zero این آسیب‌پذیری را ۵۰ روز قبل از زمان مقرر خود افشا کردند، زیرا توسعه‌دهندگان Transmission وصله مناسبی را در یک ماه گذشته در اختیار کاربران قرار ندادند.

Ormandy در گزارش منتشرشده در این رابطه می‌گوید: "اینکه سازندگان این Transmission پاسخگوی اشکالات امنیتی خود نیستند، واقعا یک موضوع ناامیدکننده است. من پیشنهاد دادم که این آسیب‌پذیری به‌صورت عمومی منتشر شود تا شاید تلنگری باشد که این سازندگان، وصله مربوطه را بلافاصله ارائه دهند. من شک دارم که آن‌ها این موضوع مهم را بدون پاسخ رها کنند اما باید منتظر شد و دید که چه پاسخی از طرف آن‌ها ارائه خواهد شد."

حمله‌ای که به منظور اثبات ادعای وجود این آسیب‌پذیری انجام شده و توسط Ormandy منتشر شده است، از یک تابع خاص در Transmission بهره‌برداری می‌کند و به کاربران اجازه می‌دهد تا برنامه BitTorrent خود را از طریق یک مرورگر وب کنترل کنند.

بهره‌برداری منتشر شده توسط آقای Ormandy بر روی مرورگرهای Chrome و فایرفاکس در سیستم‌عامل‌های ویندوز و لینوکس (Fedora و Ubuntu) کار می‌کند و او معتقد است که سایر مرورگرها و سیستم‌عامل‌ها نیز به این حمله آسیب‌پذیر هستند.

برنامه Transmission BitTorrent بر اساس معماری Server-Client کار می‌کند. در این معماری کاربران باید یک سرویس Daemon را بر روی سیستم‌های خود نصب کنند تا به یک رابط مبتنی بر وب در مرورگرهای محلی خود دسترسی داشته باشند. Daemon نصب‌شده بر روی سیستم کاربر در مرحله بعدی با یک سرور ارتباط برقرار می‌کند تا فایل‌های موردنظر را از طریق مرورگر و با استفاده از درخواست‌های JSON RPC بارگیری یا بارگذاری کند.

Ormandy متوجه شد که یک روش هک به نام حمله Domain Name System Rebinding می‌تواند از این پیاده‌سازی بهره‌برداری کند و به هر وب‌سایت مخربی که کاربر از آن بازدید می‌کند، اجازه می‌دهد که یک کد مخرب را از راه دور و با کمک سرویس Daemon نصب‌شده بر روی کامپیوتر کاربر اجرا کند.

این نقص از این واقعیت سرچشمه می‌گیرد که می‌توان سرویس‌های نصب‌شده در Localhost را برای برقراری ارتباط با وب‌سایت‌های فرد دیگری دست‌کاری کرد.

یک مقام رسمی از توسعه‌دهندگان Transmission به ArsTechnica گفته است که وصله مربوطه هر چه سریع‌تر منتشر می‌شود اما تاریخ دقیقی ذکر نکرده است.

منبع: thehackernews مترجم: سحر علیزاده

فریب کاربران به دانلود باج‌افزار با استفاده از ارزرمزی جعلی

مهاجمان با استفاده از روش‌های مهندسی اجتماعی، از افزایش بازدید ارزهای‌رمزی بهره‌برداری می‌کنند. این بهره‌برداری از طریق ارزرمزی جعلی بنام SpriteCoin صورت می‌گیرد. SpriteCoin باج افزاری است که برای فریب کاربران زودباور استفاده شده است. مهاجمان پشت پرده SpriteCoin جهت افزایش علاقه کاربران به ارزهای‌رمزی بر روی forumهای آنلاین تبلیغ می‌کنند ،

سپس تشویق می‌کنند تا آنان با دانلود بسته نرم‌افزار کیف پول، از پیشنهاد سکه اولیه (Initial Coin Offering) یک ارزرمزی جدید استفاده کنند.

هنگامی که برنامه دانلود شد، کاربران را وادار می‌کند تا گذرواژه‌ای ایجاد کنند. این گذرواژه برای دانلود BlockChain باجافزار SpriteCoin استفاده شده است. هدف واقعی برنامه پس از رمز کردن فایل‌های قربانی با پسوند encrypted. و تغییرنام آن فایل‌ها، ارائه یک یادداشت باج، تقاضای 0.3 مونرو، تقریبا ۹۱ دلار در زمان انتشار است. حمله باجافزار SpriteCoin حمله مخربانه خاصی است و به رمز کردن فایل‌ها محدود نشده است. کسانی که تصمیم می‌گیرند تا باج را پرداخت کنند، مشکلات بیشتری خواهند داشت. باجافزار در طول فاز رمزگشایی، بدافزاری را دانلود می‌کند. این بدافزار فعال‌سازی دوربین وب، تجزیه و تحلیل کلیدهای کیبورد، سرقت نام کاربری و رمز عبور را انجام می‌دهد. حملات SpriteCoin از تکنیک‌های مهندسی اجتماعی تأثیرگذار استفاده می‌کنند تا کاربران را فریب دهند. بسیاری از کاربران با انتظار کسب سود از یک ارزرمزی جدید، مورد حمله واقع می‌شوند. با توجه به این که حمله نسبتاً ساده است، نباید جای تعجب باشد که حملات بیشتر در مورد ارزهای‌رمزی جعلی در آینده دیده شود. با وجود محبوبیت ارزهای‌رمزی، کاربران باید همیشه وضعیت را ارزیابی کنند خصوصا زمانی که ارزهای‌رمزی جدید از منابع نامشخص می‌آیند. یک جستجوی سریع در موتورهای جستجو می‌تواند در تعیین قانونی بودن یک ارزرمزی جدید کمک کند. فقدان وب سایت قانونی یا هر خبری از منابع معتبر، باید یک خط قرمز برای کاربران باشد. کاربران همچنین باید از کلیک کردن بر روی لینک‌های تبلیغاتی محصولات و سرویس‌هایی که بیش از حد خوب به نظر می‌رسند، اجتناب کنند.

منبع: trendmicro گردآوری: معصومه خیری

نمایش موقعیت پایگاه‌های نظامی محرمانه با استفاده از نقشه حرارتی منتشر شده توسط ردیاب تناسب اندام

هر یک از ما اکنون دارای حداقل یک دستگاه هوشمند متصل به اینترنت هستیم، که این پرسش را برجسته‌تر می‌سازد؛ دستگاه هوشمند شما چقدر در مورد شما می‌داند؟

در طول آخر هفته، برنامه محبوب ردیابی تناسب اندام Strava با افتخار «نقشه حرارتی ۲۰۱۷» را منتشر کرد که فعالیت‌های کاربران آن در سراسر جهان را نشان می‌دهد، اما متاسفانه این نقشه چیزهایی که نباید را نشان داد؛ موقعیت‌های پایگاه‌های نظامی آمریکا در سراسر جهان!

برنامه Strava که به‌عنوان یک برنامه «شبکه‌ی اجتماعی برای ورزشکاران» عرضه می‌شود، نقشه حرارتی جهانی را در دسترس عموم قرار داد که این نقشه موقعیت تمام دوچرخه سواری‌ها، دویدن‌ها، شنا کردن‌ها و اسکی کاربران آن را نشان می‌دهد، که این اطلاعات توسط تلفن‌های همراه هوشمند و دستگاه‌های پوشیدنی مانند Fitbit آن‌ها جمع‌آوری شده است.

از آنجایی که Strava برای ردیابی مسیرها و موقعیت‌های کاربران طراحی شده است، ناتان روسر، پژوهش‌گر دانشگاه بین‌المللی آسیای مرکزی (IUCA) نشان داد که این برنامه ممکن است به‌صورت ناخواسته موقعیت برخی از نیروهای نظامی در سراسر جهان، به‌ویژه برخی از نیروهای مخفی آمریکا را نقشه‌برداری کند.

با مجموع یک میلیارد فعالیت وارد شده در نقشه فعالیت Strava، این برنامه اطلاعات بسیار مفیدی از سراسر جهان را دارا می‌باشد.

با وجود این که نقشه فعالیت Strava از ماه نوامبر سال ۲۰۱۷ میلادی در دسترس عموم قرار داشته است، روسر اخیرا متوجه شده است که این نقشه شامل مسیرهای تناسب اندام سربازان و عوامل ارتش در مکان‌های محرمانه، از جمله پایگاه‌های نظامی آمریکا در افغانستان و سوریه، یک پایگاه مشکوک سازمان سیا در سومالی و حتی منطقه ۵۱ می‌باشد.

این نقشه علاوه بر پایگاه‌های نظامی آمریکا، همچنین پایگاه هوایی RAF Mount Pleasant انگلیس را در جزایر فالکلند، دریاچه Macphee و دریاچه جزیره Gull را نشان داد. پایگاه‌های روسی نیز توسط داده‌های Strava نشان داده شده‌اند.

همچنین کارشناسان امنیتی پایگاه‌های نظامی حساس آمریکا در سومالی، افغانستان و سوریه، پایگاه‌های مخفی روسیه در اوکراین، یک پایگاه موشکی مخفی در تایوان و نیز پایگاه NSA در هاوایی را کشف کردند.

روسر گفت که این نقشه او را قادر می‌سازد تا مسیرهای منظم پیاده‌روی افراد نظامی را پیدا کند، که این خبر بدی برای امنیت است، زیرا آن‌چه که اطلاعات «الگوی زندگی» را قابل اطمینان می‌کند، مخفی نگه داشتن آن از سایر نقاط جهان می‌باشد.

روسر گفت: «اگر سربازان نیز از این برنامه مانند مردم عادی استفاده کنند، روشن کردن ردیابی آن هنگام انجام تمرین، می‌تواند بسیار خطرناک باشد. این مسیر ویژه مانند مسیر پیاده‌روی منظم به نظر می‌رسد.»

آیا Strava باید کاملا برای این افشاسازی متهم شود؟

Strava گفت که نقشه حرارتی آن تنها براساس داده‌های عمومی موجود است و این شرکت یک حالت خصوصی ارائه می‌دهد که کاربران را قادر می‌سازد به اشتراک‌گذاری داده‌ها در خارج از برنامه را خاموش کنند.

با این حال، به‌نظر می‌رسد بسیاری از افراد نظامی که از این برنامه استفاده می‌کنند، اطلاعات محرمانه را به‌صورت عمومی به اشتراک می‌گذارند که این موضوع وحشتناک است.

یک پژوهش‌گر امنیتی به واشنگتن‌پست گفت که این داده‌های در دسترس قرار گرفته حتی می‌تواند به نیروهای دشمن کمک نماید تا یک «حمله به نیروهای آمریکایی در داخل یا اطراف پایگاه‌ها» برنامه‌ریزی کنند.

آن‌چه که این موضوع را وخیم‌تر می‌سازد، این است که برخی از کارشناسان راه‌هایی را نیز برای شناسایی نقشه حرارتی Strava، شناسایی افراد و موقعیت مکانی که در آن تمرین می‌کنند، پیدا کرده‌اند.

Strava به کاربران خود یادآوری کرده است که می‌توانند خدمات موقعیت مکان این برنامه را غیرفعال کنند و این نقشه شامل فعالیت‌های خصوصی یا مناطق خصوصی نمی‌شود.

Strava در بیانیه‌ای گفت: «نقشه حرارتی جهانی ما، یک نمای کلی و ناشناس از بیش از یک میلیارد فعالیت بارگذاری شده بر روی پلتفرم ما را نشان می‌دهد. فعالیت‌هایی که با عنوان خصوصی علامت‌گذاری شده و مناطقی که توسط کاربر به‌صورت خصوصی تعریف شده باشند، حذف خواهند شد. ما متعهد هستیم تا به مردم در درک بهتر تنظیمات خود کمک کنیم تا آن‌ها بتوانند آن‌چه را که به اشتراک می‌گذارند، کنترل کنند.»

این رویداد یک یادآوری بزرگ برای مردم به‌منظور غیرفعال کردن خدمات به اشتراک‌گذاری موقعیت مکانی برای همه چیز است، به‌ویژه افرادی که در نقاط حساس یا اطراف آن کار می‌کنند.

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir

علاوه بر این، ارتش نیز باید محدود کردن استفاده از تلفن‌های همراه و دستگاه‌های پوشیدنی هوشمند را در مناطق حساس در نظر گرفته و همچنین اهمیت حریم خصوصی را به سربازان خود آموزش دهد.

منبع: thehackernews

افزایش تولید باج‌افزار در سال ۲۰۱۷ نسبت به سال‌های دیگر

گزارش‌های اواخر سال گذشته توسط شرکت امنیتی MalwareBytes در آمریکا نشان می‌دهد که باج‌افزارها، آگهی‌افزارها و بدافزارهایی که ارزرمز را به کمک توان پردازشی مرورگر کابران استخراج می‌کنند، در سال ۲۰۱۷ برای مخربان اینترنتی محبوب بوده‌اند.

داده‌های جمع‌آوری شده توسط محصولات امنیتی نشان-دهنده رشد تقریبی در همه گروه‌های مخربانه بوده است، لذا سال ۲۰۱۷، سالی موفقیت‌آمیز برای تولیدکنندگان بدافزار، هکرهای توسعه دهنده وبسایت‌های فیشینگ و دیگر گروه‌های مخربانه اینترنتی بوده است.

بر اساس گزارش بخش بدافزار MalwareBytes، در سال ۲۰۱۷ حملات باج‌افزارها بر علیه کاربران بیش از ٪۹۳ افزایش داشته حال آنکه استفاده از آن‌ها درزمینه کسب‌کار ٪۹۰ افزایش داشته است. ماه September پرتحرک‌ترین ماه سال بوده است، درحالی‌که در دوره بین دو ماه July تا September نسبت به سال ۲۰۱۶ در میزان حملات باج‌افزارها رشدی ۷۰۰ درصدی دیده می‌شود. این شرکت بیان کرد که بیشتر باج‌افزارهای تشخیص داده شده در سال قبل، از خانواده‌های WannaCry، Locky، Cerber و GlobeImposter بوده است.

اگر این موضوع را به یاد بیاوریم که سه باج‌افزار بزرگ WannaCry، NotPetya و BadRabbit که ده‌ها هزار سیستم را در سراسر دنیا آلوده کرده بودند در سال ۲۰۱۷ بوجود آمده‌اند، مشاهده باج‌افزار در لیست تهدیدهای مهم در گزارش‌های MalwareBytes چندان شگفت‌انگیز نیست. با وجود این، باج‌افزارهایی که شروع به تکثیر خودشان می‌کردند زیاد مشکل بزرگی نبوده و اکثر این آلودگی‌ها توسط کمپین‌های عمومی جاسوسی و کیت‌های توسعه (Exploit Kits) بوجود آمده بودند.

بااین‌که میزان آلودگی افزایش داشته است اما شرکت MalwareBytes بیان می‌کند که در اواخر سال ۲۰۱۷ بدلیل کاهش مشاهده تحرکات باج‌افزارها و فایل‌های مخربانه قبلی و جدید ، نفوذ و تسلط باج‌افزارها کاهش پیدا کرده است.

منبع: Beepingcomputer مترجم : ابوالفضل علیقلی‌وند

وصله شدن آسیب‌پذیری‌های بحرانی شبکه‌ی مجازی خصوصی (VPN) سیسکو

روز دوشنبه سامانه‌های سیسکو وصله‌ای را برای رفع یک آسیب‌پذیری امنیتی بحرانی در راهکار امنیت لایه‌ی انتقال وی‌پی‌ان خود که تجهیزات امنیتی سازگار نامیده می‌شود، منتشر کرد. به گفته‌ی یکی از مشاوران امنیتی سیسکو، این آسیب‌پذیری می‌تواند به یک مهاجم ناشناس و از راه دور اجازه دهد تا کد از راه دور را بر روی دستگاه‌های آسیب‌دیده اجرا نماید.

این آسیب‌پذیری تقریبا ۱۲ محصول سیسکو، اعم از ۳ هزار سری از تجهیزات امنیتی صنعتی، سری ASA ۵۵۰۰-X از دیواره‌های آتش نسل بعدی و دیواره‌ی آتش ابر V۱۰۰۰ASA را تحت تاثیر قرار می‌دهد. این اشکال که با شناسه‌ی CVE-۲۰۱۸-۰۱۰۱ ردیابی می‌شود، بالاترین امتیاز CVSS یعنی ۱۰ را دریافت کرد. سیسکو اعلام کرد که هیچ راه‌حلی برای این اشکال وجود ندارد.

با توجه به توصیه‌ی امنیتی منتشر شده، «این آسیب‌پذیری ناشی از تلاش برای آزاد کردن دو برابر بخشی از حافظه، زمانی‌که قابلیت Webvpn در دستگاه سیسکو ASA فعال است، می‌باشد. مهاجم می‌تواند با ارسال چندین بسته‌ی ایجاد شده‌ی XML به یک رابط کاربری پیکربندی webvpn بر روی سامانه‌ی آسیب‌دیده، از این آسیب‌پذیری بهره‌برداری کند. این بهره‌برداری به مهاجم اجازه می‌دهد تا کد دلخواه را اجرا کرده و کنترل

کامل سامانه را به دست آورد یا منجر به بارگذاری مجدد دستگاه آسیب‌دیده شود.»

کارشناسان امنیتی به‌دلیل ماهیت بحرانی این اشکال، در اولین فرصت وصله‌هایی را برای شرکت‌های تحت تاثیر قرار گرفته معرفی خواهند کرد.

جیسون گاربیس، مدیر اجرایی کارگروه نرم‌افزار محور امنیت ابری گفت: «وی‌پی‌ان‌های متداول مانند سیسکو یک پورت باز به اینترنت را ارائه می‌دهند، بنابراین هر کاربری می‌تواند از راه دور به آن متصل شود.» او گفت، این آسیب‌پذیری دسترسی مهاجم به یک شبکه‌ی شرکتی را فراهم خواهد کرد.

گاربیس گفت: «صدها هزار دستگاه سیسکو در سراسر جهان به‌کار گرفته می‌شوند. هیچ راه‌حلی وجود ندارد، سازمان‌ها باید به‌صورت دستی تمام کارگزارهای وی‌پی‌ان سیسکو ASA خود را به‌منظور رفع این آسیب‌پذیری شناسایی و وصله کنند.»

سیسکو گفت، درحالی‌که این آسیب‌پذیری بسیاری از دستگاه‌های ASA را تحت تاثیر قرار می‌دهد، تنها آن‌هایی که قابلیت «webvpn» را فعال کرده‌اند، آسیب‌پذیر هستند. مدیر سامانه می‌تواند با بررسی این موضوع که نسخه‌ی نرم‌افزار سیسکو ASA خود «۹,۲,۴,۲۵» و یا بالاتر است، از آسیب‌پذیر بودن دستگاه خود جلوگیری کند.

سیسکو در توصیه‌ی امنیتی خود گفت که از آگاهی عمومی در مورد این آسیب‌پذیری مطلع است، اما از این موضوع که این آسیب‌پذیری در دنیای واقعی مورد بهره‌برداری قرار گرفته باشد، اطلاعی ندارد.

سیسکو کشف این آسیب‌پذیری را به سدریک هالبرن، پژوهش‌گر گروه NCC نسبت داد. هالبرن قرار است روز جمعه، در کنفرانس امنیت رایانه‌ی REcon در بروکسل، بلژیک در مورد کشف خود صحبت کند.

منبع: news.asis.io

وجود یک آسیب‌پذیری بحرانی در کارگزار وب مورد استفاده در بیش از ۱۰۰ محصول سامانه‌ی کنترل صنعتی

در یک مولفه که توسط بیش از ۱۰۰ سامانه‌ی کنترل صنعتی (ICS) مورد استفاده قرار می‌گیرد، یک آسیب‌پذیری بحرانی پیدا شده است که می‌تواند به یک مهاجم راه دور اجازه دهد تا کد دلخواه خود را اجرا کند.

این آسیب‌پذیری مولفه‌ی کارگزار وبِ محصول CODESYS WebVisu شرکت 3S-Smart را تحت تاثیر قرار می‌دهد، این محصول به کاربران اجازه می‌دهد تا رابط‌های انسان-دستگاهِ کنترل‌های منطقی قابل برنامه‌ریزی (PLCs) را در یک مرورگر وب ببینند.

بر اساس وب‌گاه CODESYS، محصول WebVisu در ۱۱۶ PLC و رابط‌های انسان-دستگاه ۵۰ فروشنده از جمله Schneider Electric، WAGO، Hitachi، Advantech، Beck IPC، Berghof Automation، Hans Turck، NEXCOM مورد استفاده قرار گرفته است.

S-Smart۳ در یک مشاوره‌نامه توضیح داد: «یک درخواست کارگزار وب جعلی ممکن است باعث سرریز بافر شود و سپس مهاجم می‌تواند کد دلخواه خود را در کارگزار وب اجرا کند و یا با ایجاد اختلال در کارگزار وب شرایط حمله‌ی منع سرویس توزیع‌شده را فراهم کند.»

این فروشنده می‌گوید، با این‌که هیچ مدرکی مبنی‌بر بهره‌برداری از این آسیب‌پذیری در سراسر جهان وجود ندارد، اما حتی یک مهاجم با مهارت این توانایی را دارد که از راه دور از این اشکال بهره‌برداری کند.

این آسیب‌پذیری با شناسه‌ی CVE-۲۰۱۸-۵۴۴۰ ردیابی می‌شود و در نمره‌دهی CVSS امتیاز ۹,۸ را دارد. نسخه‌ی ۱,۱,۹,۱۹ و نسخه‌های پیش از آن کارگزارهای وب CODESYS v ۲,۳ که به صورت مستقل یا بخشی از سامانه‌ی زمان اجرای CODESYS روی تمام نسخه‌های ویندوز اجرا می‌شوند، تحت تاثیر این آسیب‌پذیری قرار دارند. این اشکال در نسخه‌ی ۱,۱,۹,۱۹ که بخشی از

نسخه‌ی CODESYS ۲,۳,۹,۵۶ نیز است، وصله شده است.

با این‌که شرکت 3S-Smart می‌گوید که از این حفره‌ی امنیتی هیچ بهره‌برداری صورت نگرفته است، اما به سازمان‌ها توصیه می‌کند که اطمینان حاصل کنند که دسترسی به کنترل‌کننده‌ها را بسیار محدود کنند تا شبکه کمتر در معرض خطر قرار بگیرد و همچنین از دیواره‌های آتش و شبکه‌های خصوصی مجازی استفاده کنند. این شرکت همچنین یک مقاله‌ی سفید درباره‌ی امنیت در برنامه‌های کنترل صنعتی منتشر کرد.

وجود آسیب‌پذیری در مولفه‌های CODESYS غیرمعمول نیست. ماه آوریل گذشته نیز، استارتاپ امنیت سایبری CyberX چندین آسیب‌پذیری بحرانی را در کارگزار وب CODESYS کشف کرده بود. اخیرا شرکت SEC Consult یک آسیب‌پذیری در یکی از مولفه‌های CODESYS را گزارش داد که PLCهای شرکت WAGO و احتمالا دیگر شرکت‌ها را در معرض حمله قرار می‌دهد.

موتور جست‌وجوی Shodan درگاه ۲۴۵۵ را رصد کرده است که از سال ۲۰۱۴ میلادی مخصوص پروتکل CODESYS است. این موتور جست‌وجو در حال حاضر بیش از ۵۶۰۰ سامانه را نشان می‌دهد از طریق این درگاه در دسترس هستند، بیش‌تر این سامانه‌های آسیب‌پذیر در آمریکا، آلمان، ترکیه، چین و فرانسه قرار دارند.

منبع: news.asis.io

مجهز شدن پردازنده‌های AMD به محافظت دربرابر بهره‌برداری‌های مشابه Spectre

پردازنده‌های جدید Zen 2 و مدل‌های آینده‌ی AMD شامل محافظت‌هایی در برابر Spectre و سایر بهره‌برداری‌های مشابه آن خواهند بود، این غول فن‌آوری روز سه‌شنبه درآمد خود را در سال ۲۰۱۷ میلادی اعلام کرد.

مدیر عامل AMD، لیسا سو، تاکید کرد که پردازنده‌های این شرکت در برابر حملات Meltdown آسیب‌پذیر نیستند و اجرای یکی از انواع حملات Spectre روی محصولات آن بسیار سخت است.

وی تشریح کرد: «برای نوع اول Spectre ما همچنان در زمینه‌ی مقابله با این نوع حمله به صورت فعال با شرکای تجاری و کاری خود کار می‌کنیم، که از جمله‌ی این همکاری‌ها، وصله‌های سامانه‌عامل است که انتشار آن‌ها آغاز شده است. ما همچنان معتقدیم که بهره‌برداری از نوع دوم Spectre در پردازنده‌های AMD بسیار دشوار است، با این حال وصله‌های میکروکد پردازنده‌ها را به همراهبه‌روزرسانی‌های سامانه‌عامل ارائه می‌دهیم تا اقدامات بیشتری برای مقابله انجام دهیم.»

وی خاطرنشان کرد که در بلند مدت شرکت قصد دارد در تمام هسته‌های پردازنده‌ی آینده، حفاظت‌هایی برای بهره‌برداری‌های مشابه Spectre ارائه دهد. این حفاظت‌ها در طراحی پردازنده‌های Zen 2 اخیر پیاده‌سازی شده است که انتظار می‌رود سال آینده در دسترس باشد.

شرکت AMD از درآمد ۵/۳۳ دلاری در سال ۲۰۱۷ گزارش داد که در مقایسه با سال گذشته ۲۵ درصد افزایش یافته است. با این حال، این شرکت هشدار داد که بهره‌برداری‌های Spectre و Meltdown می‌توانند روی درآمد شرکت تاثیر منفی داشته باشند.

این شرکت اظهار داشت: «آسیب‌پذیری‌های امنیتی واقعی یا مشاهده شده در محصولات AMD ممکن است AMD را در معرض تبلیغات مغایر و مضر قرار دهد، به نام تجاری و اعتبار آن صدمه بزند، و نیز می‌تواند به کسب‌وکار و نتایج مالی AMD آسیب بزند.»

اینتل نیز به مشتریان اطلاع داد که روی پردازنده‌هایی کار می‌کند که شامل محافظت‌های داخلی در برابر حملات Spectre و Meltdown خواهند بود.در ضمن، وصله‌های نرم‌افزار و میکروکد موجود، موجب بروز مشکلاتی برای بسیاری از کاربران شده است، که باعث شده تا زمانی که این مشکلات حل شوند شرکت‌ها به‌روزرسانی‌ها را متوقف سازند و راه‌حل‌های مقابله‌ای را غیرفعال کنند.

منبع: news.asis.io

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

با توجه به افزایش تعداد حوادث امنیتی رایانه‌ای و لزوم وجود مراکز تخصصی دانشگاهی برای پشتیبانی و رفع نیازهای پژوهشی جامعه در این حوزه، و با انگیزه ارتقای دانش و توان مهندسی در حوزه امنیت سیستم‌های کامپیوتری و پردازش اطلاعات و انتقال نتایج به جامعه، آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی، از اواخر سال ۱۳۹۴ فعالیت خود را آغاز نمود و از زمان آغاز فعالیت، اقدامات زیر صورت گرفته است:

۱. ارزیابی امنیتی و انجام آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای

تست نفوذ یا ارزیابی امنیتی روشی است که توسط آن قادر می‌توان آسیب‌پذیری‌های موجود در نرم‌افزارها، شبکه، وب‌سایت و بانک‌های اطلاعاتی خود را شناسایی کرده و پیش از آنکه نفوذگران واقعی به سیستم وارد شوند، امنیت سیستم خود را افزایش داد. این روش با استفاده از ارزیابی جنبه‌های مختلف امنیتی کمک می‌کند تا با کاهش دادن ریسک‌های امنیتی موجود، احتمال نفوذ غیرمجاز به شبکه کاهش یابد.

۲. مشاوره در زمینه امن‌سازی سامانه‌ها و شبکه رایانه‌ای

با توجه فعالیت‌های مختلفی که آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی در زمینه زیرساخت‌های امنیتی مانند پیاده‌سازی سیستم مدیریت امنیت اطلاعات، پیاده‌سازی انواع ابزارهای امنیتی، تدوین الگوهای امنیتی داشته است، کارشناسان این مرکز دارای دیدی جامع نسبت به مسایل امنیتی با توجه به اهداف استراتژیک و راهبردی و با توجه به موجودیت‌های هر سازمان دارند و آماده ارائه راهکار امنیت اطلاعات و شبکه در تمامی سازمان‌ها با ویژگی‌ها و موجودیت‌های مختلف می‌باشند. خدمات و راهکارهای امنیت اطلاعات و سیستم‌های کامپیوتری این مرکز، با بررسی وضعیت فعلی سیستم‌های موجود در سازمان آغاز می‌شود و با بهره‌گیری از تکنولوژی و تخصص روز، با معماری و اجرای راه حل‌های جامع ایمن سازی سیستم های کامپیوتری ، کامل می گردد.

۳. برگزاری دوره‌های آموزشی در زمنیه دانش امنیتی برای سازمان‌ها و نهادهای زیربط

امنیت فضای سایبری فرآیندی است و باید آن را گام به گام و به روز جلو برد بنابراین آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقائ دانش امنیت اطلاعات متولیان فاوای سازمان‌ها و نیز به منظور تربیت نیروهای متخصص چندین دوره کارگاه‌های آموزشی برگزار نموده است.

۴. تولید نرم‌افزارهای امنیتی

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقا سطح امنیت فضای سایبری به تولید نرم افزارهای امنیتی اقدام نموده است که عبارت است از: سامانه تحلیل‌گر فایل‌های اجرائی (ستفا)، دیده‌بان، رادار

۵. پاسخگویی به حملات

آزمایشگاه و مرکز تخصصی آپای دانشگاه محقق اردبیلی به محض دریافت درخواستی مبنی بر وقوع حملاتی تحت وب، زیرساخت‌های شبکه، سامانه‌های اداری و حملات بدافزاری در اسرع وقت با سازمان مورد حمله ارتباط برقرار می‌کند و با شناسایی نوع و فرایند حمله، مولفه‌های مربوط به آسیب‌پذیری سیستم، راهکارهای مناسب برای جلوگیری از حمله مجدد و بهره‌برداری از ضعف سیستم را ارائه می‌دهد همچنین با شناسایی نقاط ضعف سیستم و ارائه مشاوره برای رفع این نقاط آسیب‌پذیر سیستم را در مقابل حملات جدید مقاوم می‌سازد.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

www.cert.uma.ac.ir

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir