خبرنامه مرکز تخصصی آپای دانشگاه ایلام

شماره هفتم - فروردین ماه ۱۳۹۷

- جدیدترین اخبار مربوط به حوزه امنیت
- معرفی جدیدترین بد افزارها
- هشدارها و راهنمایی های امنیتی
- اخبار مرکز تخصصی آپای دانشگاه

آسیب‌پذیری بحرانی در سرویس QoS تجهیزات سیسکو

فهرست

هشدار مرکز ماهر در خصوص آسیب‌پذیری بحرانی در سرویس QoS تجهیزات سیسکو ۳

هشدار مرکز ماهر به کاربران بهره‌بردار از روترهای Mikrotik ۴

اطلاعیه مرکز ماهر درخصوص حواشی مطرح شده در فضای مجازی در مورد اپلیکیشن ((روبیکا)) ۵

بدافزار Gold Dragon ۶

هشدار مرکز ماهر در خصوص آسیب‌پذیری بحرانی در سرویس QoS تجهیزات سیسکو

اخیرا #آسیب_پذیری با هدف سرویس Quality of Service در سیستم عامل IOS و IOS XE تجهیزات #سیسکو توسط این شرکت گزارش شده است. این آسیب پذیری با مشخصه‌ی #CVE_۲۰۱۸_۰۱۵۱، امکان اجرای کد از راه دور را برای حمله کننده فراهم می کند. این آسیب پذیری به دلیل وجود ضعف "#عدم بررسی مرزحافظه تخصیص داده شده" در کد های سیستم عامل IOS به وجود آمده است.

مهاجم می تواند با بهره برداری از این آسیب پذیری، بسته های مخرب را به پورت UDP:۱۸۹۹۹دستگاه های آسیب پذیر ارسال کند. هنگامی که بسته ها پردازش می شوند، یک وضعیت سرریز بافر قابل بهره برداری رخ می دهد. یک بهره برداری موفق می تواند به مهاجم اجازه دهد تا کد دلخواه را با سطح دسترسی بالا در دستگاه اجرا کند و یا با reload دستگاه باعث توقف سرویس دهی دستگاه شود.

دستگاه های آسیب پذیر

سرویس و پورت آسیب‌پذیر بصورت پیش‌فرض بر روی تجهیزات سیسکو فعال نیست و تنها تجهیزاتی که از قابلیت #DMVPN و نسخه‌ای بروز نشده از سیستم عامل سیسکو استفاده می کنند تحت تاثیر این آسیب‌پذیری هستند.

با استفاده از دستور show udp می توانید از غیر فعال بودن این پورت اطمینان حاصل کنید.

جهت مسدود سازی این آسیب‌پذیری می توانید با استفاده از #ACL، دسترسی به پورت UDP ۱۸۹۹۹ تجهیز را مسدود نمایید.

هشدار مرکز ماهر به کاربران بهره‌بردار از روترهای Mikrotik

با توجه به اطلاعیه اخیر شرکت #میکروتیک در خصوص روترهای میکروتیک با سیستم عامل RouterOS v۶٫۳۸٫۵ به قبل، نسخه جدیدی از #بات‌نت Hajime فعال شده و در مقیاس وسیع اقدام به نفوذ و سوءاستفاده از این روترها می نماید.این بات با اسکن آی پی های عمومی در اینترنت و یافتن روترهای با پورت های باز ۸۲۹۱(نرم افزار winbox) و ۸۰ (وب)، از طریق سوءاستفاده از آسیب‌پذیری ملقب به ChimayRed اقدام به نفوذ و بهره‌برداری از منابع روترهای آسیب‌پذیر می‌نماید.

برای ایمن سازی روترها در برابر این آسیپ پذیری رعایت نکات زیر الزامی است:

#سیستم_عامل روتر را بروزرسانی کنید.

سرویس مدیریت تحت وب روتر را غیرفعال کرده یا دسترسی به آن را به شبکه داخلی خود محدود نمایید. توجه داشته باشید در صورت فعال بودن سرویس و وجود آلودگی در شبکه داخلی، همچنان امکان آلودگی روتر وجود دارد.

جهت غیرفعال سازی سرویس وب در قسمت IP Service سرویس WWW را غیر فعال نمایید.

اگر در شبکه خود هات اسپات دارید Webfig را غیرفعال کنید.

در قسمت IP Service و Allowed-From دسترسی مدیریتی به روتر را فقط به شبکه ای خاص یا آی پی خاص بدهید.

MikroTik

اطلاعیه مرکز ماهر درخصوص حواشی مطرح شده در فضای مجازی در مورد اپلیکیشن ((روبیکا))

در پی طرح سوالات و مباحث مطرح شده در فضای مجازی در خصوص اپلیکیشنی با عنوان ((نرم افزار چند رسانه ای اندرویدی روبیکا)) و تاکید وزیر محترم ارتباطات و فناوری اطلاعات مبنی بر بررسی موضوع توسط مرکز ماهر، این اپلیکیشن مورد تحلیل دقیق این مرکز قرار گرفت. در بررسی آخرین نسخه ((۱.۰.۸)) از این برنامه مشاهده شد کدهای منبع نسخه اندرویدی تلگرام بصورت کامل در این نرم افزار قرار گرفته است. دلیل این امر استفاده از واسط گرافیکی مبتنی بر Fragments پیاده سازی شده در نرم افزار تلگرام بوده و بخش عمده باقی مانده اساسا بی استفاده مانده است. از نظر عملکردی نیز قابلیت های شبکه های اجتماعی مشابه تلگرام در این نرم افزار پیاده سازی نشده است و صرفا خدمات ارائه شده توسط این اپلیکیشن براساس قابلیت WebView اندروید و شامل ارائه محتوای شماری از وب سایت ها است. در نتیجه بر اساس بررسی صورت گرفته می توان بیان داشت که: این نرم افزار حریم خصوصی کاربران را نقض نمی کند. این نرم افزار دسترسی به محتوای اطلاعات سایر اپلیکیشن ها از جمله تلگرام را ندارد (اساسا با توجه به تکنولوژی application security sandbox سیستم عامل اندروید، اجرای اپلیکیشن ها در فضایی ایزوله انجام شده و برنامه ها امکان دسترسی مستقیم به داده های یکدیگر را ندارند) کدهای منبع نسخه اندرویدی تلگرام بصورت کامل در این نرم افزار قرار داده شده اما تنها از برخی کلاس های واسط گرافیکی آن در برنامه بهره برداری شده است و سایر قسمت ها قابل حذف هستند.

نسخه مورد بررسی اساسا قابلیت شبکه اجتماعی یا پیام رسان نظیر تلگرام را ارائه نمی کند.

درخصوص استفاده از نرم افزارهای متن باز با لایسنس GPL و عدم رعایت تعهدات حقوقی مربوط به آن، متاسفانه این موضوع در محصولات داخلی امری رایج بوده و در این محصول نیز مورد توجه واقع نشده است.

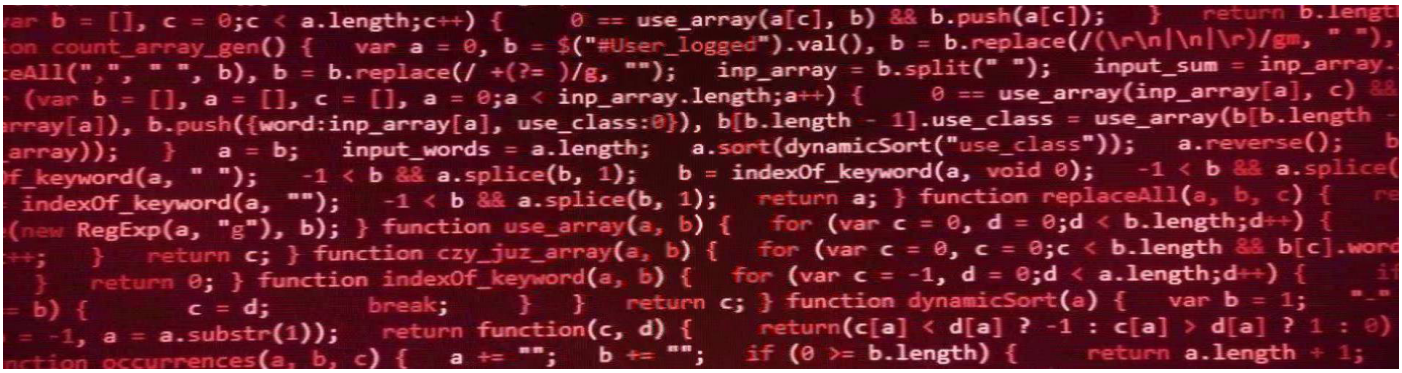
درخصوص استفاده از مجوز (certificate) امضای دیجیتال با نام شرکت گوگل لازم به توضیح است که این مجوز بصورت خودامضا (self signed) بوده و جزییات آن در محیط توسعه اندروید بطور پیش فرض به نام شرکت گوگل ثبت شده است و لازم بود شرکت توسعه دهنده نرم افزار این مشخصات را پیش از انتشار عمومی تغییر می داد.

درخصوص لوگوی اپلیکیشن، اظهارنظر در این مورد در صلاحیت این مرکز نیست.

بدافزار Gold Dragon

گروه پژوهشی تهدیدات پیشرفته McAfee اخیراً گزارشی را منتشر کرده است که بیان می کند یک حمله بدون فایل ، سازمان های برگزارکننده المپیک زمستانی پیونگ چانگ را که در کره جنوبی برگزار می شود، هدف حمله خود قرار داده است. این حمله از قرار دادن یک اسکریپت PowerShell بر روی سیستم قربانی استفاده می کند که کانالی را به سمت سرور مهاجم برای جمع آوری اطلاعات پایه در سطح سیستم ایجاد می کند.

تحلیل گران McAfee در ۲۴ دسامبر ۲۰۱۷، یک بدافزار با نام Gold Dragon به زبان کره ای را مشاهده کردند. به گفته McAfee در حال حاضر این بدافزار، مرحله دوم این حملات به بازی های المپیک است که گروه پژوهشی تهدیدات پیشرفته McAfee آن را در ۶ ژانویه ۲۰۱۸ کشف کرد. اسکریپت PowerShell که در کمپین های المپیک مورد استفاده قرار می گرفت، یک عامل قدیمی مبتنی بر چارچوب Empire PowerShell بود که یک کانال رمز شده را به سمت سرور مهاجم ایجاد می کرد. با این حال، این اسکریپت، نیاز به ماژول های اضافی دارد تا به عنوان یک درب پشتی کاملاً کارآمد اجرا شود. علاوه بر این، اسکریپت PowerShell دارای مکانیزمی نیست که فراتر از یک وظیفه ساده زمان بندی شده دوام بیاورد. Gold Dragon مکانیزم ماندگاری بسیار قوی تری نسبت به اسکریپت مخرب PowerShell اولیه دارد و مهاجم را قادر می سازد تا سیستم هدف را خیلی بیشتر مورد حمله قرار دهد. همان روزی که کمپین المپیک آغاز شد، Gold Dragon دوباره ظاهر شد. بدافزار Gold Dragon قابلیت های گسترده ای برای به دست آوردن اطلاعات از سیستم هدف و ارسال نتایج آن به یک سرور کنترل دارد. اسکریپت اجرایی PowerShell فقط قابلیت جمع آوری داده های اولیه مانند نام کاربری، دامنه، نام دستگاه و پیکربندی شبکه را داشت که تنها برای شناسایی قربانیان و راه اندازی بدافزارهای پیچیده تری علیه آنها قابل استفاده بود.



مرکز تخصصی آپای دانشگاه ایلام

پست الکترونیکی cert@ilam.ac.ir

وب سایت cert.ilam.ac.ir