هک وب‌کم در IOS/macOS تنها با یک کلیک بر روی لینک جعلی

خلاصه‌ی خبر:

طبق آخرین گزارش‌ها، وب‌کم در iOS/macOS را می‌توان تنها با یک کلیک بر روی لینک جعلی هک کرد!

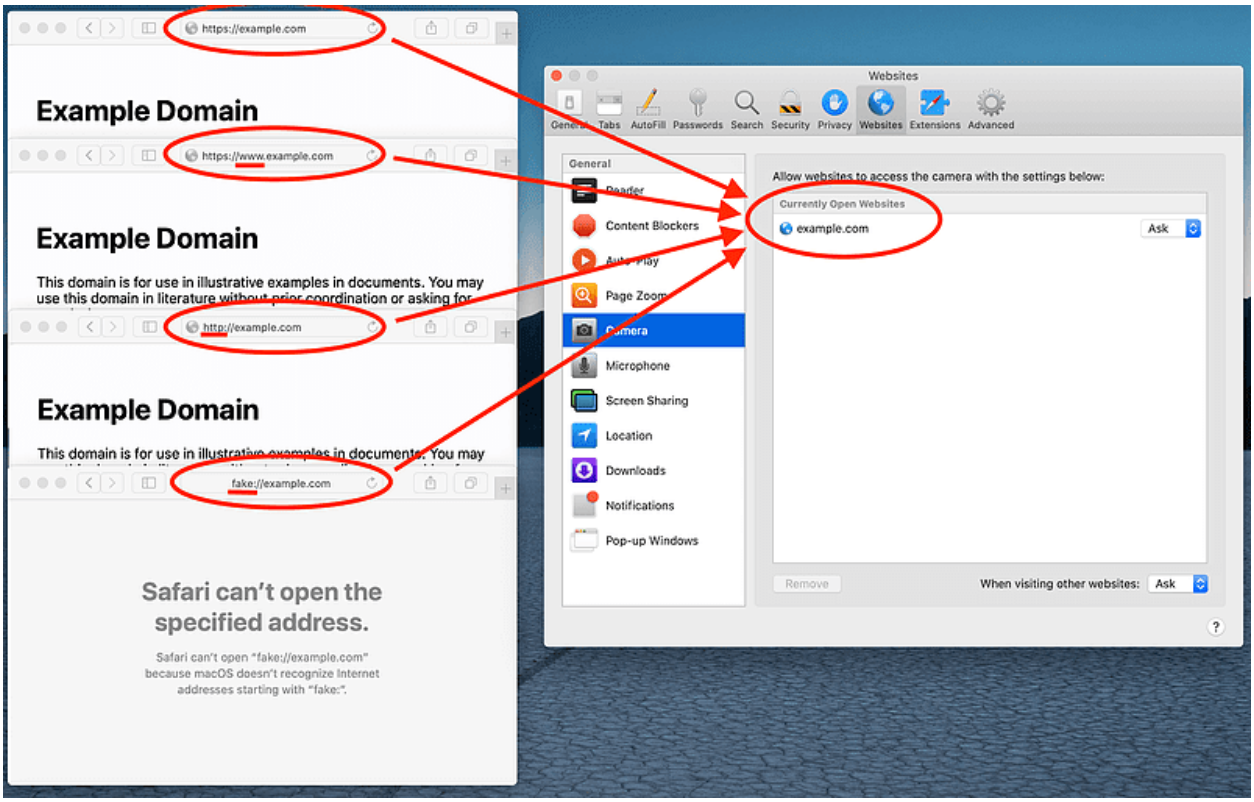
به‌دلیل مدل امنیتی دوربین‌های iOS و MacOS، برای هر برنامه باید به صورت دستی مجوز دسترسی اختصاص داده‌شود اما برنامه‌های خود اپل مانند Safari بصورت پیش‌فرض به دوربین دسترسی دارند.

محقق امنیتی، Ryan Pickren، هفت آسیب‌پذیری جدید را در مرورگر Safari کشف کرد که به مهاجمین اجازه‌ی دسترسی به دوربین، میکروفون یا مکان‌یاب شما را می‌دهند، و در برخی موارد رمزهای عبور را نیز ذخیره می‌کنند.

طبق گزارش‌های منتشر شده، وب‌کم در iOS/macOS را می‌توان تنها با یک کلیک بر روی لینک جعلی هک کرد و کافی‌ست مهاجم کاربر را به بازدید از یک لینک وادارد، آنگاه می‌تواند دوربین iOS/macOS کاربران را از طریق نقص روزصفرم موجود در Safari هک کند.

به‌دلیل مدل امنیتی دوربین‌های iOS و MacOS، برای هر برنامه باید به صورت دستی مجوز دسترسی اختصاص داده‌شود اما برنامه‌های خود اپل مانند Safari بصورت پیش‌فرض به دوربین دسترسی دارند.

محقق امنیتی، Ryan Pickren، هفت آسیب‌پذیری جدید را در مرورگر Safari کشف کرد که به مهاجمین اجازه‌ی دسترسی به دوربین، میکروفون یا مکان‌یاب شما را می‌دهند، و در برخی موارد رمزهای عبور را نیز ذخیره می‌کنند.

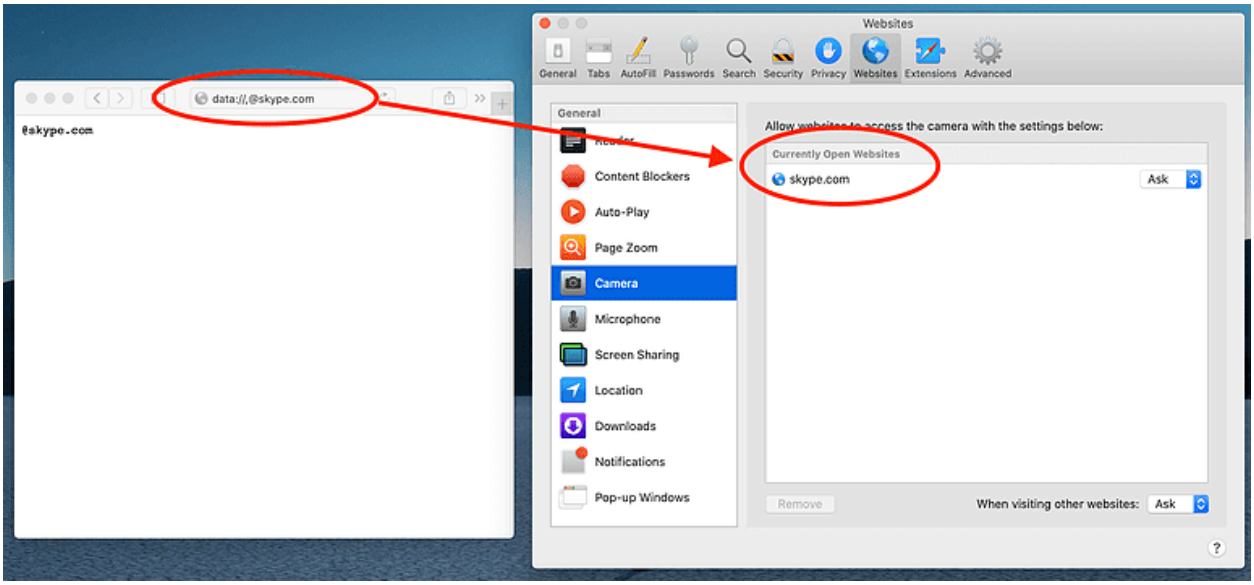


Ryan Pickren با بیان اینکه Safari از روش origin برای ردیابی وب‌سایتهای باز استفاده نمی‌کند، گفت: "من متوجه‌شده‌ام که احتمالاً Safari یک تجزیه‌کننده Generic URI Syntax را در برابر

همه صفحات و زبانه‌های باز اجرا می‌کند تا نام میزبان URLها را بدست آورد و سپس برخی از تجزیه‌های اضافی را روی آن‌ها انجام می‌دهد".

بهره‌برداری از نقص‌ها برای دسترسی به دوربین

وی با استفاده از" javascript: data: and about " شروع به بهره‌برداری از این نقص‌ها کرد که با شکست مواجه شد اما هنگام تجزیه‌ی file: که برای دسترسی از راه دور یا FTP تعیین شده است، (file: //host.example.com/Share/path/to/file.txt) را در نظر گرفت.



Safari آن را به عنوان یک URI با پرونده‌ی نرمال تجزیه می‌کند، و این محقق می‌گوید: "صفحه در واقع این URI را معتبر پذیرفته و همان مطالب را مجدداً بارگیری می‌کند. این بدین معنی‌ست که من فقط با استفاده از این ترفند واقعا ساده، دامنه‌ی سند را تغییر دادم." (CVE-2020-3885)

بنابراین اکنون مرورگر Safari فکر می‌کند که وب‌سایت متصل‌شده skype9.0com است و با باز کردن فایلهای محلی، مهاجمین می‌توانند اسکریپتی مخرب را اجرا کنند و به دوربین، میکروفون و اشتراک‌گذاری صفحه دسترسی پیدا کنند.

وی یک اشکال دیگر با شناسه‌های (CVE-2020-9784 و CVE-2020-3887) یافت تا جلوگیری از بارگیری خودکار در مرورگر Safari را دور بزند.

با استفاده از آدرس *blob: //skype.com* می‌توان یک پنجره‌ی پاپ‌آپ را ایجاد کرد و از آن برای اجرای JavaScript دلخواه استفاده می‌شود.

امتحان‌کردن تمام این اشکالات زنجیره‌ای، می‌تواند دسترسی به دوربین iOS/macOS، میکروفون یا مکان‌یاب و در برخی موارد حتی رمزهای ذخیره شده را تضمین کند.

شناسه‌های این هفت آسیب‌پذیری در زیر آورده شده‌اند:

CVE-2020-3852

CVE-2020-3864

CVE-2020-3865

CVE-2020-3885

CVE-2020-3887

CVE-2020-9784

CVE-2020-9787

البته باید گفت همه این آسیب‌پذیری‌ها در به‌روزرسانی‌های ژانویه و مارس وصله شدند و محقق ۷۵ هزار دلار باگ‌بانتی برای گزارش این نقص‌ها دریافت می‌کند.

منبع:

https://gbhackers.com/ios-macos-webcam/