بسمه تعالی

بررسی هفت آسیب‌پذیری روز صفرم در مرورگر Safari

گزارش آسیب‌پذیری

دوربین iPhone یا MacBook می‌تواند تنها با بازدید از یک سایت هک شود. مراجعه به یک سایت (نه تنها سایت‌های مخرب، بلکه سایت‌های مجاز که ناآگاهانه تبلیغات مخربی را نمایش می‌دهند) با استفاده از مرورگر Safari می‌تواند به مهاجمان از راه دور اجازه دهد به طور مخفیانه به دوربین، میکروفون یا مکان دستگاه و در برخی مواقع رمزهای عبور ذخیره شده دسترسی پیدا کنند.

اخیراً شرکت اپل یک پاداش ۷۵ هزار دلاری به یک هکر اخلاقی به نام Ryan Pickren پرداخت کرد که عملاً عملیات هک را شرح داده و به شرکت کمک کرده است تا در مجموع هفت آسیب پذیری جدید را پیش از آن که هر مهاجمی بتواند از آن‌ها استفاده کند، ترمیم کند. این اصلاحات در یک سری به‌روزرسانی نسخه‌های spanning در مرورگر Safari نسخه ۱۳.۰.۵ (منتشر شده در ۲۸ ژانویه ۲۰۲۰) و نسخه Safari ۱.۱۳ (منتشر شده در ۲۴ مارس ۲۰۲۰) اعمال شد.

به گفته Pickren، اگر یک وب‌سایت مخرب نیاز به دسترسی دوربین داشته باشد، تنها باید خود را به عنوان یک وب‌سایت معتبر کنفرانس ویدیویی مانند Skype یا Zoom جا بزند.

استفاده از زنجیره‌ی سه نقض گزارش شده‌ی Safari باعث می‌شود سایت‌های مخرب خود را به جای سایت‌های مجاز که قربانی به آن اعتماد دارد جا بزند و با سوءاستفاده از مجوزهایی که توسط قربانی به دامنه مورد اطمینان اعطا شده بود، به میکروفون یا دوربین دسترسی پیدا کنند.

۱ یک زنجیره بهره‌برداری برای سوءاستفاده از مجوزهای مربوط سایت‌های Safari

مرورگر Safari به هر سایت مجوزهای دسترسی خاصی مانند دوربین، میکروفون، موقعیت مکانی و موارد دیگر را می‌دهد. به گفته Skype، این مسئله باعث می‌شود با هر بار راه‌اندازی برنامه در وب سایت‌های شخصی، بدون درخواست مجوز دسترسی کاربر، دسترسی به دوربین آسان شود. اما در مورد iOS استثناءهایی وجود دارد. هنگامی که برنامه‌های شخص ثالث برای دسترسی به دوربین به مجوز کاربران نیاز دارند، مرورگر Safari می‌تواند بدون اعلان سریع به دوربین یا گالری تصاویر دسترسی پیدا کند. در واقع، دسترسی نادرست با اعمال زنجیره‌ای از بهره‌برداری از نواقص که به هم متصل شده‌اند باعث می‌شود مرورگر،

برنامه URL [۱] را تجزیه کرده و تنظیمات امنیتی را بر اساس هر وب‌سایت دستکاری کند. این روش فقط در وب‌سایت‌هایی که در حال حاضر باز هستند عمل می‌کند. Pickren خاطرنشان کرد این که برنامه URL کاملاً نادیده گرفته شود، مشکل ساز است زیرا بسیاری از آن‌ها مانند file:، javascript:، یا data: دارای نام میزبان معنادار نیستند.

به عبارت دیگر، Safari نمی‌تواند بررسی کند که آیا در صورت رعایت سیاست مشابه در وب‌سایت‌ها، می‌توان به سایت دیگری که در ابتدا به مجوز نیاز ندارد دسترسی پیدا کرد یا خیر. در نتیجه، وب سایتی مانند «https://example.com» و همتای مخرب آن «fake://example.com» می‌توانند با داشتن مجوزهای مشابه متوقف شوند.

بنابراین با بهره‌گیری از کندی تجزیه نام میزبان Safari، استفاده از فایل URI [۲] (به عنوان مثال، file:///path/to/file/index.html)، برای فریب مرورگر در تغییر نام دامنه، با استفاده از جاوا اسکریپت امکان‌پذیر خواهد بود.

مرورگر Safari تصور می‌کند که کاربر در سایت skype.com است و مهاجم می‌تواند از این طریق جاوا اسکریپت مخرب را بارگذاری کند؛ سپس هنگامی‌که کاربر پرونده HTML محلی را باز کند، دوربین، میکروفون و اشتراک گذاری صفحه به خطر می‌افتند.

این گزارش نشان می‌دهد حتی رمزهای عبور ساده نیز می‌توانند با این روش سرقت شوند زیرا Safari از همان رویکرد برای شناسایی وب‌سایت‌هایی که در آن پر کردن خودکار رمز عبور لازم است، استفاده می‌کند. علاوه بر این با باز کردن یک سایت قابل اعتماد به عنوان یک Pop up [۳] و در نتیجه استفاده از آن برای بارگیری یک فایل مخرب، بارگیری خودکار می‌تواند دور زده شود.

---

[۱] محتوای وب شامل برنامه (پروتکل)، میزبان (دامنه) و پورت URL که برای دسترسی به آن استفاده می‌شود می‌باشد. دو شیء فقط وقتی که برنامه، میزبان و پورت آن‌ها با هم یکسان باشد، دارای مبداء یکسان هستند.

[۲] URI مخففuniform resource identifier است. با توجه به معنی لغوی آن URI در واقع تعیین کننده هویت یکنواخت منابع آنلاین است.

[۳] پاپ آپ(Pop-Up) ها تبلیغاتی هستند که بدون اجازه کاربر باز می‌شوند. آن‌ها اغلب آزار دهنده بوده و ممکن است حاوی لینک‌های آلوده و دامی برای کاربران باشند.

به همین ترتیب، یک blob[۴] URI (به عنوان مثال blob: //skype.com) می‌تواند برای اجرای کد جاوا اسکریپت دلخواه مورد سوءاستفاده قرار بگیرد و از آن برای دسترسی بدون اجازه و مستقیم به دوربین قربانی استفاده شود.

در کل در این گزارش هفت آسیب‌پذیری مختلف روز صفرم در Safari بررسی شده است:

- CVE-2020-3852: ممکن است یک برنامه URL هنگام تعیین مجوز چندرسانه‌ای برای یک وب‌سایت به اشتباه نادیده گرفته شود.
- CVE-2020-3864: ممکن است یک فیلد شیء DOM[۵]، اصل امنیتی منحصر به فردی نداشته باشد.
- CVE-2020-3865: ممکن است یک فیلد شیء DOM در سطح بالا به اشتباه ایمن تلقی شود.
- CVE-2020-3885: ممکن است یک فایل URL به طور نادرست پردازش شود.
- CVE-2020-3887: ممکن است مبداء بارگیری یک فایل به طور نادرست مرتبط شده باشد.
- CVE-2020-9784: ممکن است یک iframe مخرب از تنظیمات بارگیری وب‌سایت دیگری استفاده کند.
- CVE-2020-9787: ممکن است یک برنامه واکشی URL حاوی خط (-) و نقطه (.) هنگام تعیین مجوز چند رسانه‌ای برای یک وب‌سایت در مجاورت یکدیگر به اشتباه نادیده گرفته شود.

به کاربران Safari توصیه می‌شود مرورگر را به روز نگه داشته و اطمینان حاصل کنند که وب‌سایت‌ها فقط به آن دسته از تنظیماتی که برای عملکرد آن‌ها ضروری است مجوز دسترسی می‌دهند.

۲ مراجع

[1] https://thehackernews.com/2020/04/hacking-iphone-macbook-camera.html

[۴] کلمه BLOB مخفف عبارت Binary Large Object است و به فایل‌های عظیم مانند یک عکس یا یک فایل صوتی و غیره دلالت دارد که به دلیل سایز متفاوت این فایل‌ها، باید آن‌ها را با روش‌های خاصی آپلود، دانلود یا ذخیره در دیتابیس کرد.

[۵] یک مدل و ساختار درختی از تمام عناصر HTML درون یک صفحه وب است که در آن عناصر HTML به عنوان اشیاء در نظر گرفته می‌شوند.