禪

هک با فایلهای MP3

یک آهنگ به تنهایی میتواند گوشی های آندرویدی را هک کند

به تازگی رخنه جدیدی در Stagefright توسط پژوهشگران آزمایشگاه امنیتی Zimperium zLabs شناسایی گردیده است. این رخنه جدید زمانی که کاربر یک فایل MP3 را باز میکند، تلفن آندرویدی او را در معرض خطر قرار میدهد .

اگر به یاد داشته باشید در ماه جولای گروهی از محققان امنیتی اعلام کردند، رخنههای متعددی را در سیستمعامل آندروید شناسایی کردهاند که به هکرها اجازه میدهد با ارسال پیامهای کوتاه سیستم کاربران را مورد حمله قرار دهند . آن رخنهها در Stagefright شناسایی شده بود. دو روز پیش همان گروه امنیتی اعلام کردهاند که دو باگ جدید را در Stagefright شناسایی کردهاند که به هکرها اجازه میدهد کاربران را فریب داده تا به بازدید از سایتهای مخربی که شامل کدهای مخرب مرتبط با فایلهای چندرسانهای صوتی و تصویری است، مبادرت ورزند.

مطلب پیشنهادی: چگونه تلفنهای آندرویدی را رمزنگاری کنیم

بنابر گزارشها اکسپلویت جدید شناسایی شده طیف گستردهای از دستگاههای آندرویدی را تحت تأثیر خود

قرار میدهد، به طوریکه این رخنه روی دستگاههای آندرویدی که از نسخه 1.0 تا نسخه 5 این سیستمعامل استفاده میکنند فعال است . رخنه جدید روی ابزار Stagefright نگارش 2.0 شناسایی شده است. این ابزار برای پردازش متادیتاهای درون فایلهای ویدویی MP4 یا فایلهای صوتی MP3 مورد استفاده قرار میگیرد . اجرای یک پیشنمایش از یک آهنگ یا ویدیو باعث اجرای این اکسپلویت شده، به طوری که به یک هکر اجازه میدهد از راه دور به اجرای کدها بپردازد . این رخنه همچنین روی برنامههای ثالثی تأثیرگذار است که از کتابخانه Stagefright برای پخش فایلهای صوتی و تصویری استفاده میکنند .

در زمان نگارش این مقاله این رخنه در رده آسیبپذیریهای بحرانی و جدی شناخته نشده است . هنوز هیچ کد مفهومی برای اثبات این رخنه منتشر نشده است، در نتیجه وصلهای هم برای آن ارائه نشده است، اما شرکت سازنده Stagefright زمانی که نرمافزار خود را بهروزرسانی کند وصلهای را برای آن ارائه خواهد کرد . محققان این باگ را در تاریخ 15 آگوست به گوگل اطلاع دادهاند، بر همین اساس گوگل مطابق با زمانبندیهای خود یک وصله امنیتی برای نکسوسها را در هفته دوم اکتبر ارسال خواهد کرد . سازندگان گوشیهای دیگر همچون HTC، شیائومی، سامسونگ و سونی باید بهروزرسانیهای مورد نیاز را خود شخصا تولید کنند، اما زمانبندی دقیقی از سوی این شرکتها ارائه نشده است . آزمایشگاه Zimperium چند هفته پیش ایمیلی را برای گوگل ارسال کرده بود و در آن ایمیل اعلام کرده بود که نزدیک به 8 باگ را در سیستمعامل آندروید شناسایی کرده است. این آزمایشگاه همچنین گزارش بیش از ده باگ در Stagefright را برای گوگل ارسال کرده بود . دریک مدیرعامل این شرکت امنیتی به سایت مادربرد گفته است، تعدادی از رخنههای شناسایی شده در رده آسیبپذیریهای بحرانی و تعداد کمی از آنها در رده آسیبپذیریهای با درجه امنیتی کم شناخته میشوند . سخنگوی این شرکت اعلام کرد که نمیتواند در خصوص این آسیبپذیریهای شناسایی شده توضیح بیشتری ارائه کند، به دلیل اینکه هر یک از این آسیبپذیریهای شناسایی شده یک خطر بالقوه را برای کاربران به وجود میآورند . او در پایان صحبتهای خود اعلام کرد به احتمال زیاد آسیبپذیریهای بیشتری در موتور Stagefright وجود دارند که هنوز شناسایی نشدهاند .

بنابر گزارشهای منتشر شده، جدیدترین نسخه از سیستمعامل آندروید، مارشمالو از این رخنه در امان است، اما تنها تعداد کمی از دستگاهها مجهز به این سیستمعامل هستند . متأسفانه برای دستگاههای قدیمیتر که وصلهای برای آنها ارائه نمیشود، این رخنه به قوت خود باقی خواهد بود، مگر آنکه دارندگان این گوشیها خود شخصا نسخه جدیدی از آندروید را نصب کنند . اگر رخنهای مشابه مورد اخیر روی بستر اینترنت شناسایی میگشت، میتوانست فاجعهآمیز باشد . به دلیل اینکه تنها نیاز داشت کاربر URL که شامل یک فایل مخرب است را مورد بازدید قرار دهد . در نتیجه در حالی که به نظر میرسید یک آهنگ عادی در حال پخش است فایل مخرب به سادگی اجرا میشد.

نویسنده :
حمیدرضا_تائبی
منبع :
نکستوب
دسته بندی:
امنیت
تاریخ انتشار :
01:40 - 14/07/1394
برچسب:
آندروید - هک - Stagefright - آهنگ - گوشی

منبع: https://www.shabakeh-mag.com/security/1820