禪

آسیبپذیری جدید در کروم

هک شدن دستگاههای اندرویدی در یک چشم بر هم زدن، امکانپذیر شد

در چند ماه گذشته، گوگل به شدت مشغول برطرف کردن آسیبپذیریهای امنیتی بوده است که در سیستمعامل محبوب اندروید، شناسایی شدهاند؛ هرچند آسیبپذیریهای مختلفی در این سیستمعامل برطرف شدهاند؛ اما هنوز، تعداد بسیار زیادی از آسیبپذیریهای ناشناخته باقی مانده است و به راحتی میتوانند توسط هکرها مورد سو استفاده قرار گیرد. هکرها به تازگی، حفره امنیتی جدیدی را در مرورگر کروم دستگاههای اندرویدی، شناسایی کردهاند.

این حفره جدید به هکرها اجازه میدهد با استفاده از آخرین نسخه مرورگر کروم، به دستگاههای اندرویدی نفوذ کنند و امنیت این دستگاهها را به خطر بیندازند. این حمله روی نسخههای مختلف سیستمعامل اندروید امکانپذیر است. گوانگ گونگ، محقق شرکت امنیتی Quihoo 360 برای اولین بار، خبر شناسایی این حفره امنیتی را در کنفرانس PacSec که در توکیو ژاپن برگزار شد، اعلام کرد؛ البته این کارشناس امنیتی به جزییات این آسیبپذیری هیچگونه اشارهای نکرد؛ اما هکرها با استفاده از نسخه 8 جاوا اسکریپت، توانایی نفوذ به اسمارتفون کاربران و دسترسی کامل به اسمارتفونها را خواهند داشت. تاکنون آسیبپذیریهای مختلفی روی سیستمعامل اندروید شناسایی شدهاند، اما نکتهای که این آسیبپذیری را متمایز از نمونههای مشابه میکند، به یک مرحلهای بودن آن باز میگردد. در بسیاری از حملات هکری، هکرها با استفاده از چند آسیبپذیری، سعی میکنند به دستگاه کاربر نفوذ کنند؛ اما در آسیبپذیری جدید، تنها در یک مرحله کاربر قربانی این رخنه میشود. به گفته Dragos Ruiu برنامهریز کنفرانس PacSec هر زمان کاربری سعی کند تا با استفاده از مرورگر کروم دستگاه همراه خود، به بازدید از سایتهای مخربی بپردازد که از نسخه 8 جاوااسکرپیت استفاده میکنند، هکرها با استفاده از آسیبپذیری موجود در این نسخه از جاوااسکرپیت، توانایی نصب برنامه مخرب روی دستگاه کاربر را خواهند داشت و در این حالت، کاربر هیچ گونه کنترلی روی برنامه نصب شده ندارد . Ruiu

میگوید ما این آسیبپذیری را روی دستگاه مشخصی آزمایش کردیم؛ اما به احتمال زیاد این رخنه، پتانسیل آسیب رساندن به هر دستگاهی را با استفاده از موتور جاوااسکریپت، خواهد داشت . گوانگ گونگ، محقق شرکت Quihoo 360 نزدیک به سه ماه زمان صرف کرده است تا بتواند چنین رخنهای را شناسایی کند . Dragos Ruiu برنامهریز کنفرانس PacSec، آسیبپذیری موجود و نحوه ورود هکرها به دستگاه قربانی را روی یک Nexus 6 آزمایش کرد و نتیجه را به مخاطبان این کنفرانس نشان داد . Ruiu درباره رخنه شناسایی شده توسط گوانگ گونگ میگوید: «امروزه، هکرها برای آنکه بتوانند به مجوزهای مدیریتی سطح سیستمی دست پیدا کنند و برنامههای مختلف را روی اسمارتفون کاربران بارگذاری کنند، به چندین آسیبپذیری نیاز دارند تا بتوانند از آنها بهرهبرداری کنند؛ در حالی که آسیبپذیری شناسایی شده توسط گونگ متفاوت است و در یک مرحله کاربر را قربانی میکند .» Ruiu میگوید : «تیم امنیتی گوگل، از این باگ اطلاع پیدا کردهاند و به احتمال زیاد، قبل از آنکه جزییات مربوط به این رخنه به صورت علنی منتشر شود، گوگل وصله لازم را ارائه میدهد . در زمان نگارش این مقاله، گونگ به سایت رجیستر گفت : "آسیبپذیری موجود، تمامی نسخههای اندروید که از آخرین نسخه مرورگر کروم استفاده میکنند را تحت تأثیر قرار داده است ."

گوگل هنوز به این آسیبپذیری کشف شده هیچ گونه واکنشی نشان نداده است؛ هر چند آسیبپذیری شناسایی شده توسط گونگ، یک رخنه مهم به شمار میرود؛ اما متأسفانه گونگ نمیتواند مطابق با برنامه bug bounty program که از سوی گوگل ارائه شده است و به کارشناسان امنیتی در خصوص پیدا کردن رخنه در سیستمعامل کروم و مرورگر کروم جایزهای پرداخت میکند، جایزه خود را دریافت کند . گوگل برای شناسایی آسیبپذیریها در این دو محصول جایزهای از 500 دلار تا 5 هزار دلار پرداخت میکند . محققان امنیتی در یک سال گذشته، مجموعهای از آسیبپذیریهای بحرانی همچون رخنه Stagefright که روی میلیونها دستگاه همراه تأثیرگذار بوده است را شناسایی کردند . Stagefright 2 رخنه خطرناک دیگری بود که همه دستگاههای اندرویدی را در معرض خطر قرار داد .

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
10:04 - 29/09/1394
برچسب:
اندروید - هک اندروید

□□□□□ منبع: https://www.shabakeh-mag.com/security/2474