

Help us keep your account safe.

Verify your identity by entering the phone number associated with your Twitter account.

[Why am I being asked for this information?](#)

Hint: Your phone number ends in

Submit

آسیب‌پذیری خطرناکی که چند ماه پیش در شبکه اجتماعی توییتر شناسایی شده بود سرانجام روز پنجم مارس ترمیم شد. هکرها از طریق آسیب‌پذیری فوق‌قادر بودند از مکانیزم امنیتی توییتر عبور کنند و به حساب‌های کاربری قفل شده دسترسی پیدا کنند. ساختار توییتر به گونه‌ای است که به این شبکه اجتماعی اجازه می‌دهد حساب‌های کاربری را به دلایل امنیتی قفل کند. این کار به منظور حفاظت از حساب‌ها به مرحله اجرا در می‌آید.

در تمامی شبکه‌های اجتماعی منجمله توییتر زمانی که حسابی قفل می‌شود، مالک حساب باید هویت واقعی خود را از طریق شماره تلفن و آدرس ایمیل به اثبات برساند تا بتواند مجدداً از حساب خود استفاده کند. اما آرون اولگر، پژوهشگر امنیتی کشف کرد سازوکاری که توییتر برای قفل کردن حساب‌ها از آن استفاده می‌کند آسیب‌پذیری بوده و می‌توان از آن عبور کرد. برای بهره‌مندی از این آسیب‌پذیری هکر باید حساب کاربری هدف را به اسمارت‌فون خود اضافه کند. این پژوهشگر اعلام کرده است: «حساب کاربری قفل شده‌ای را با استفاده از صفحه تنظیمات به آی‌فون خود افزودم. در ادامه برنامه توییتر را روی آی‌فون نصب کردم و به همین سادگی موفق شدم به حساب کاربری مسدود شده به طور کامل دست پیدا کنم، این اتفاق در شرایطی رخ داد که حساب فوق‌روی سایت توییتر همچنان قفل بود.» در این مکانیزم حمله پژوهشگر فوق‌نسخه iOS برنامه توییتر را برای دستیابی به بخش تنظیمات و به دست آوردن آدرس ایمیل و شماره تلفنی که برای باز کردن حساب قفل شده به آن نیاز بود مورد استفاده قرار داد. آسیب‌پذیری فوق‌به ویژه برای هک‌رهایی سودمند است که گواهی‌نامه‌های مربوط به یک حساب کاربری را به سرقت برده‌اند و از طرفی تمایلی ندارند تا حساب فوق‌به واسطه رفتارهای مشکوک قفل شود.

مطلب پیشنهادی



بیگانه‌ای پرسه می‌زند شماره 186

سرقت و فاش‌سازی اطلاعات 58 میلیون کاربر در توییتر

اولگر در وبلاگ خود نوشته است: «یک هکر با دانش لازم در ارتباط با گواهی‌نامه‌های قفل شده مربوط به یک حساب کاربری قادر است از این آسیب‌پذیری بهره‌برداری کرده و به طور کامل به پروفایل قربانی دست پیدا کند.» اولگر گزارش مربوط به این آسیب‌پذیری را نزدیک به چهار ماه پیش برای توییتر ارسال کرد و سرانجام دیروز توییتر این رخنه را ترمیم کرد. توییتر برای شناسایی رخنه‌های امنیتی خطرناک در زیرساخت‌های خود از سال 2014 میلادی برنامه پاداش در برابر باگ را روی زیرساخت HackerOne به مرحله اجرا در آورد. سایت HackerOne گزارش کرده است تا به امروز نزدیک به 600 آسیب‌پذیری در ارتباط با توییتر از سوی کارشناسان امنیتی شناسایی شده است. توییتر تاکنون بیش از 600 هزار دلار به پژوهشگران مربوطه پاداش داده است.

تاریخ انتشار:

نشانی منبع: <https://www.shabakeh-mag.com/security/7136>