

# نقص‌های امنیتی خطرناک شبکه 5G سرقت هویت کاربران را ممکن می‌کند - دیجیاتو

محمد قریشی | یکشنبه، ۳۰ آذر ۱۳۹۹

در حالی که شبکه 5G به تازگی در اختیار کاربران قرار گرفته و هنوز فاصله تقریباً طولانی تا استفاده اکثر مردم جهان از آن داریم، محققان به نقص‌های امنیتی خطرناکی پی برده‌اند که هکرها می‌توانند از آن‌ها برای سرقت هویت استفاده کنند.

بر اساس [پژوهشی جدید](#)، این آسیب‌پذیری‌ها در شبکه‌های 5G غیر مستقل کنونی و مستقل آینده وجود دارند. این گزارش که از سوی شرکت امنیت سایبری «Positive Technologies» منتشر شده، اعلام می‌کند که اکثر اپراتورهای موبایل در حال حاضر سرویس‌های 5G غیر مستقل را در اختیار کاربران قرار می‌دهند که مبتنی بر زیرساخت‌های نسل قبلی یعنی 4G LTE است.

با توجه به این آسیب‌پذیری‌ها در پروتکل‌های «Diameter» و «GTP»، شبکه‌ها در حال گذر به حالت مستقل هستند. با این حال طبق گزارش جدید این اقدام هم نمی‌تواند مانع از بروز حملات شود و همچنان کاربران شبکه 5G در معرض خطر قرار دارند.

آسیب‌پذیری‌ها در پروتکل‌های «HTTP/2» و «PFCEP» که توسط شبکه‌های مستقل 5G مورد استفاده قرار می‌گیرند، می‌توانند حمله مهاجمان برای سرقت اطلاعات پروفایل مشترکین، جعل هویت و احراز هویت جعلی را ممکن کنند.



مدیر ارشد فناوری Positive Technologies به نام «دیمیتری کورباتوف» اعلام کرد: «این خطر وجود دارد که مهاجمان از شبکه‌های مستقل 5G در هنگام استقرار و همچنین درگیری اپراتورها با آسیب‌پذیری‌های احتمالی، سوءاستفاده کنند. با توجه به این موضوع باید از همان ابتدا مشکلات امنیتی از سوی اپراتورها مورد بررسی قرار بگیرند.»

او همچنین گفت: «حمله به مشترکین می‌تواند از نظر مالی به شرکت‌ها ضرر بزند و همچنین اعتبار آن‌ها را زیر سوال ببرد که چنین موضوعی با توجه به رقابت سنگین کنونی برای ارائه سرویس‌های 5G، اهمیت بالایی دارد. با توجه به متنوع بودن این حملات، ساختار قدرتمند هسته شبکه امن‌ترین راه برای محافظت از کاربران محسوب می‌شود.»

کورباتوف با توجه به افزایش استفاده از شبکه‌های مستقل 5G و ورود آن به بخش‌های مختلف زندگی بشر، از رشد پتانسیل تخریبی این آسیب‌پذیری‌ها خبر داده. این آسیب‌پذیری‌ها می‌توانند بسیاری از صنایع از پزشکی گرفته تا حمل و نقل را با مشکل مواجه کنند.

[دیجیاتو](#)