کاربران این روترها توصیه‌های امنیتی را جدی بگیرند

۱۰ آسیب‌پذیری بحرانی در روترهای لینک‌سیس شناسایی شد

پژوهش‌گران شرکت امنیتی IOActive گزارش کرده‌اند که 10 آسیب‌پذیری جدی را در روترهای لینک‌سیس شناسایی کرده‌اند. در حالی که لینک‌سیس وصله‌های مربوطه را هنوز ارائه نکرده است، اما در مقابل به کاربران توصیه کرده است تا زمان عرضه به‌روزرسانی‌ها یکسری تهمیدات لازم را به کار گیرند.

در این پژوهش محققان شرکت IOActive روترهای مجهز به ویژگی وای‌فای هوشمند شرکت لینک‌سیس را مورد بررسی قرار داده‌اند. قابلیت وای‌فای هوشمند (Smart Wi-Fi) به مالکان روترهای فوق این توانایی را می‌دهد تا از راه دور و از طریق برنامه نصب شده روی گوشی هوشمند خود روترهای‌شان را مدیریت کرده و تنظیم کنند. شرکت لینک‌سیس گفته است، آسیب‌پذیری‌های شناسایی شده روی 25 مدل از سری‌های EA و WRT تاثیرگذار هستند.

مطلب پیشنهادی

حمله هم‌نگاره در یک قدمی کاربران
شناسایی این حمله فیشینگ برای کروم، فایرفاکس و اپرا تقریبا غیرممکن است

شرکت IOActive گفته است، مادامی که شرکت لینک‌سیس به‌روزرسانی‌های مربوطه را برای میان‌افزار دستگاه‌های آلوده عرضه نکند، جزییات مربوط به این آسیب‌پذیری‌ها را به طور عمومی منتشر نخواهد کرد. بررسی‌های انجام شده از سوی کارشناسان IOActive نشان می‌دهد اگر هکری موفق شود از این آسیب‌پذیری‌ها استفاده کند، این توانایی را به دست خواهد آورد تا یک حمله منع سرویس را پیاده‌سازی کرده، اطلاعات حساس روتر را به سرقت برده یا حتا یک درب پشتی را روی دستگاه قربانی نصب کند.

دو مورد از آسیب‌پذیری‌های شناسایی شده ممکن است به منظور پیاده‌سازی حمله منع سرویس مورد استفاده قرار گیرند. یک هکر قادر است از طریق ارسال درخواست‌های جعلی برای رابط برنامه‌نویسی روتر مانع از پاسخ‌گویی روتر یا راه‌اندازی مجدد آن شود. این دو آسیب‌پذیری نه تنها باعث بروز اختلال شدید در شبکه می‌شوند بلکه دسترسی مدیر شبکه به میان‌افزار روتر را نیز غیر ممکن می‌کنند.

مطلب پیشنهادی

کارت‌های بانکی ایمن‌تر
مسترکارت از کارت مجهز به حسگر اثر انگشت رونمایی کرد

آسیب‌پذیری دوم به منظور دور زدن احراز هویت مورد استفاده قرار می‌گیرد. آسیب‌پذیری فوق به یک هکر اجازه دسترسی به اسکریپت‌های CGI را می‌دهد. در نتیجه یک هکر به راحتی قادر خواهد بود اطلاعاتی در رابطه با میان‌افزار دستگاه، نسخه کرنل لینوکس، پردازه‌های در حال اجرا، ابزارهای USB متصل و پینWPS را جمع‌آوری کند. یک هکر حتا این توانایی را دارد تا اطلاعاتی در ارتباط با پیکربندی دیواره آتش، تنظیمات FTP و تنظیمات SMB را نیز جمع‌آوری کند.

مطلب پیشنهادی

مشکلی دیگر در ارتباط با اثرانگشت
اثرانگشتی که قفل هر گوشی هوشمندی را باز کند

پژوهش‌گران IOActive گفته‌اند: «اگر هکری به دنبال آن باشد تا به حساب روترها وارد شود، به امتیازات ویژه‌ای دست پیدا می‌کند که به او اجازه می‌دهد تا دستورات موردنظر خود را به درون میان‌افزار روتر تزریق کند. در نتیجه یک هکر قادر خواهد بود یک حساب درب پشتی را در شرایطی روی دستگاه قربانی نصب کند که او هیچ‌گاه از وجود چنین حسابی آگاه نشود.»

جستجوی انجام شده با موتور جستجوگر شادون نشان می‌دهد در حال حاضر نزدیک به هفت هزار دستگاه آسیب‌پذیر به طور مستقیم به اینترنت متصل هستند و هر لحظه ممکن است در معرض تهدید هکرها قرار گیرند.
آسیب‌پذیری‌های فوق اولین بار در ماه ژانویه شناسایی شدند و در همان ماه شرکت لینک‌سیس در جریان این آسیب‌پذیری‌ها قرار گرفت. این شرکت به کاربران خود توصیه کرده است تا زمان عرضه میان‌افزار جدید ویژگی شبکه مهمان (Guest Network) را غیرفعال کرده و گذرواژه پیش فرض دستگاه خود را تغییر دهند.

تاریخ انتشار:

02 اردیبهشت 1396

نشانی منبع: https://www.shabakeh-mag.com/security/7599