مواظب باشید: آسیب‌پذیری جدید در روترهای Netgear

دو آسیب‌پذیری جدید که در روترهای شرکت Netgear شناسایی شده‌اند به هکرها این توانایی را می‌دهند تا با در اختیار داشتن امتیازات ریشه کدهای مخرب خود را به مرحله اجرا درآورند. بدون شک این خبر خوشایندی برای دارندگان این روترها نیست.

روترهای مدل R7000 و R6400 که از جدیدترین میان‌افزارهای این شرکت استفاده می‌کنند، متاسفانه به میان‌افزارهای رخنه‌پذیری آلوده هستند که به هکرها اجازه می‌دهند تا حمله تزریق کد را به مرحله اجرا درآورند. کارشناسان امنیتی گزارش کرده‌اند که نمی‌توان آمار دقیقی در ارتباط با کاربرانی که آلوده به این آسیب‌پذیری هستند ارائه کرد. روز یکشنبه دانشگاه کارنگی ملون در بانک‌اطلاعاتی آسیب‌پذیری‌های عمومی این دانشگاه به نقل از کارشناسان امنیتی نوشت: « هکرها برای آن‌که موفق شوند حمله خود را بر مبنای این آسیب‌پذیری‌ها عملیاتی کنند، تنها باید کاربر را تشویق کنند تا از سایت آلوده‌ای بازدید کند. زمانی که کاربران کنجکاو شوند تا سایت هدف را مشاهده کنند، کدهای مخربی که روی این سایت قرار دارد و به منظور سوء استفاده از این آسیب‌پذیری طراحی شده است به مرحله اجرا در می‌آیند. در این حالت دستورات مخرب روی روترهای آلوده به این آسیب‌پذیرها همراه با امتیازات ویژه اجرا می‌شوند.»

مطلب پیشنهادی

آیا باید در انتظار یک حمله DDoS مهیب باشیم؟
۳.۲ میلیون روتر خانگی در معرض حمله قریب‌الوقوع هکرها

خبر بد این است که متاسفانه جزییات مربوط به یک آسیب‌پذیری شناسایی شده که به راحتی قابل استفاده است، به طور عمومی منتشر شده و به هر کاربری اجازه می‌دهد با اطلاع از جزییات مربوط به این آسیب‌پذیری به روترهای سایر کاربران حمله کند. برای مشاهده جزییات مربوط به این آسیب‌پذیری به آدرس Netgear R7000 - Command Injection مراجعه کنید.

پژوهشگران امنیتی هشدار داده‌اند که به احتمال زیاد آسیب‌پذیری‌های فوق در مدل‌های دیگر نیز وجود دارد. در همین ارتباط مرکز CERT به کاربرانی که از روترهای Netgear استفاده می‌کنند، پیشنهاد کرده است، مادامی که وصله‌های مربوطه برای این آسیب‌پذیری‌ها منتشر نشده است از به کارگیری این روترها خودداری کنند.

مطلب پیشنهادی

Kelihos بات‌نتی که باج‌افزار توزیع می‌کند
بات‌نتی ۸ ساله که هیچ کارشناس امنیتی نتوانسته نابودش کند!

گزارش‌هایی که در چند وقت اخیر منتشر شده است، نشان می‌دهند که هکرها به شکل کاملا هدفمندی روترهای آسیب‌پذیر را هدف خود قرار داده‌اند. به طوری که در نظر دارند این دستگاه‌ها را به بخشی از بات‌نت‌های ویژه اینترنت اشیا تبدیل کنند. اگر به خاطر داشته باشید چند روز پیش خبری در ارتباط با آلوده شدن بیش از 3.2 میلیون روتر خانگی را منتشر کردیم. در آن خبر گفتیم هکری که در پشت این قضیه قرار داشت حتا جزییات مربوط به شیوه کار خود را نیز منتشر کرد. دستگاه‌های در معرض خطر تنها به یک منظور و آن هم پیاده‌سازی حملات منع سرویس انکار شده مورد استفاده قرار می‌گیرند. حملات منع سرویس انکار شده عمدتا زیرساخت‌های متعلق به شرکت‌های فعال در زمینه سرویس‌های اینترنتی را هدف خود قرار می‌دهند.

مطلب پیشنهادی

رقابت بر سر تخریب بیشتر
رقیب بدافزار Mirai با قدرت مهیبی به میدان وارد شد

در نمونه مشابهی بات‌نت Mirai با پیاده‌سازی یک حمله بسیار سنگین منع سرویس انکار شده موفق شد شرکت داین را هدف خود قرار دهد و برای چند ساعت دسترسی به سایت‌هایی که این سرویس‌دهنده اینترنتی میزبان آن‌ها بود را با اختلال روبرو کند. همچنین در نمونه مشابهی مشترکان شرکت تاک‌تاک، اداره پست انگلستان و تعداد قابل توجهی از ساکنان آلمان (یک میلیون نفر) با عدم دسترسی به سرویس‌های اینترنت و سرویس‌هایی که روی اسمارت‌فون‌های آن‌ها فعال بود، روبرو شدند. در آن حمله روترهای شرکت Telekom به عنوان هدف هکرها مورد استفاده قرار گرفته بود.

تاریخ انتشار:

23 آذر 1395

نشانی منبع: https://www.shabakeh-mag.com/security/5895