هشدار مرکز ماهر در مورد نشت اطلاعات حساس کاربران در مسیریاب سیسکو

نویسنده : خدیجه غبیشاوی 1397-11-21 - 11:17 صبح

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای نسبت به آسیب‌پذیری تجهیزات تحت وب «سیسکو» که نشت اطلاعات حساس کاربران را به همراه دارد، هشدار داد.

به گزارش فابانیوز، مرکز ماهر با هشدار نسبت به آسیب‌پذیری‌هایی با درجه اهمیت بالا در Cisco RV۳۲۰/RV۳۲۵ اعلام کرد: «تجهیزات مسیریاب و روتر سیسکو شامل Cisco Small Business RV۳۲۰ و RV۳۲۵ Dual Gigabit Wan VPN Router دارای دو آسیب‌پذیری با درجه اهمیت بالا هستند که یکی از آنها از نوع نشت اطلاعات حساس و دیگری از نوع تزریق دستور است.»

این مرکز اوایل امسال نیز نسبت به آسیب‌پذیری گسترده تجهیزات تحت وب سیسکو هشدار داده بود.

آسیب‌پذیری نشت اطلاعات حساس

این آسیب‌پذیری با شناسه CVE-۲۰۱۹-۱۶۵۳ در رابط تحت وب تجهیزات سیسکو نهفته است و به مهاجم احراز هویت نشده راه دور، اجازه استخراج اطلاعات حساس را می‌دهد. این آسیب‌پذیری ناشی از کنترل دسترسی نامناسب URL ها است. مهاجم می‌تواند بدین وسیله به اطلاعات پیکربندی یا اشکال‌زدایی (debug) تجهیزات دست یابد.

آسیب‌پذیری تزریق دستور

این آسیب‌پذیری که شناسه CVE-۲۰۱۹-۱۶۵۲ به آن اختصاص یافته است نیز، ریشه در رابط تحت وب این تجهیزات دارد. منشاء آسیب‌پذیری، اعتبارسنجی نادرست ورودی کاربر است. مهاجم می‌توانـد با ارسال درخواست مخرب POST از این نقص بهره‌برداری کنـد. با بهره‌برداری موفق می‌توان دسـتورات دلخواه را در قالب کاربر root روی shell لینوکس تجهیزات اجرا کرد. بهره‌برداری از این آسیب‌پذیری نیازمند احراز هویت است.

کـد بهره‌برداری از آسـیب‌پـذیری‌های فوق به طور عمومی منتشـر شده است. همان طور که گفته شد، می‌توان با اسـتفاده از آسـیب‌پذیری اول، اطلاعات تجهیز از جمله اطلاعات کاربری درهم‌سازی (hash) شده را استخراج کرد. سپس می‌توان با شکستن hash، اطلاعات کاربری را به دست آورده و از آسیب‌پذیری دوم بهره‌برداری کرد.

مرکز ماهر اعلام کرد: سیسـکو برای رفع آسیب‌پذیری‌های نامبرده، به‌روزرسانی‌هایی برای سخت‌افزار تجهیزات فوق منتشر کرده است. برای مصونیت از هر دو آسیب‌پذیری باید از نسخه ۱.۴.۲.۲۰ به بالا استفاده کرد.

نسخه‌های به روزشده از اینجا قابل دریافت است.

منبع: مهر