کد خبر: ۱۰۰۵۰۴۲
یکشنبه ۲۲ اردیبهشت ۱۳۹۸ ۱۶:۵۱

مرکز ماهر اعلام کرد؛

رفع نقص بحرانی در سوئیچ‌های ۹۰۰۰ سیسکو

سیسکووصله‌های امنیتی جهت رفع ده‌ها آسیب‌پذیری در محصولات خود را منتشر کرد.

به گزارش گروه علم و فناوری ایسکانیوز، سیسکو وصله‌های امنیتی جهت رفع ده‌ها آسیب‌پذیری در محصولات خود منتشر کرده است. در میان نقص‌هایی که سیسکو برطرف ساخته است، یک آسیب‌پذیری بحرانی در سوئیچ‌های ۹۰۰۰ وجود دارد که با شناسه۱۸۰۴-۲۰۱۹- ردیابی می‌شود و رتبه۹.۸ را دریافت کرده است.

این نقص در مدیریت کلیدی نرم‌افزار سوئیچ سری‌های ۹۰۰۰ حالت زیرساخت مرکزی برنامه‌کاربردی سیسکو (() ۹۰۰۰) که بخشی از نرم‌افزار سیسکو است، وجود دارد.
شرکت‌ها از برای اعمال و کنترل برنامه‌های کاربردی در زیرساخت‌های خود، از جمله موانع چندکاره خود به همراه سیاست‌های سازگار (از نظر تئوری باعث افزایش امنیت و دسترس‌پذیری بالا می‌شود) استفاده می‌کنند. متأسفانه سیسکو دارای یک جفت کلید پیش‌فرض داخلی برای تابع مدیریت کلید پوسته امن نرم‌افزار () است، بنابراین این نقص به مهاجم اجازه می‌دهد این جفت کلید را کشف و از راه دور و به عنوان یک کاربر قانونی به یک دستگاه آسیب‌پذیر سری‌های ۹۰۰۰ متصل شود.

به عبارتی، یک مهاجم می‌تواند با بازکردن یک اتصال از طریق ۶ به دستگاه هدف، با استفاده از ابزار کلیدی استخراج‌شده، سواستفاده کند. این نقص بااستفاده از اتصالات ساخته‌شده از طریق ۴ قابل سواستفاده نیست.

به گفته سیسکو، این نقص در تمامی دستگاه‌هایی که سوئیچ‌های سری‌های ۹۰۰۰ در حالت زیرساخت مرکزی برنامه‌کاربردی () که نسخه نرم‌افزاری - پیش از ۱۴.۱ (۱) را اجرا می‌کنند، وجود دارد.

سیسکو با انتشار به‌روزرسانی نرم‌افزاری، این نقص را برطرف ساخته است. سیسکو اطلاعاتی راجع به راه‌حل‌های مقابله با این آسیب‌پذیری و سواستفاده‌های عمومی از آن ندارد، لذا به کاربران توصیه می‌کند به آخرین نسخه نرم‌افزاری به‌روزرسانی کنند.

سیسکو همچنین وصله‌هایی برای بیش از ۲۰ آسیب‌پذیری با شدت بالا که نرم‌افزار) ، ،()) و))، مسیریاب‌های ۳۲۰ و ۳۲۵، سری‌های ۷۸۰۰ و ۸۸۰۰، نرم‌افزار)) و سوئیچ‌های ۹۰۰۰ را تحت‌تأثیر قرار می‌دهد، منتشر ساخته است.
سواستفاده از این آسیب‌پذیری‌ها به مهاجمان اجازه افزایش امتیاز، ایجاد انکار سرویس در دستگاه‌های متأثر، سرقت نشست‌ها، دسترسی به یک داشبورد، دورزدن احرازهویت گواهینامه، استقرار یک نشست یا کشف کلیدهای خصوصی یک دستگاه متأثر می‌دهد.

از جمله این آسیب‌پذیری‌های با شدت بالا، یک آسیب‌پذیری دیگر (۱۸۵۹-۲۰۱۹-)، این بار در فرایند احرازهویت نرم‌افزار سوئیچ‌های ، است . دلیل وجود این آسیب‌پذیری، نادیده گرفته‌شدن فرایند احرازهویت توسط است. مهاجم می‌تواند با تلاش برای اتصال به دستگاه

آسیب‌پذیر از طریق ، از این آسیب‌پذیری سواستفاده کند. سواستفاده‌ی موفق از این آسیب‌پذیری به مهاجم اجازه می‌دهد به عنوان یک کاربر مدیریتی، در صورتی که اعتبارنامه‌ها تغییر نیافته باشند، به پیکربندی دسترسی یابد.

آسیب‌پذیری با شدت بالای دیگر (۱۶۳۵–۲۰۱۹–) که در گوشی‌های وجود دارند، می‌توانند منجر به سقوط آن‌ها شده و قابلیت‌های یک گوشی تجاری را کسب کنند. این نقص در برنامه تماس تلفنی پروتکل پیاده‌سازی نشست () برای سری‌های ۷۸۰۰ و ۸۸۰۰ وجود دارد. این آسیب‌پذیری ناشی از مدیریت خطای ناکامل، زمانی که داده‌های درون یک بسته‌ی تجزیه می‌شوند، است. یک مهاجم می‌تواند با ارسال بسته‌ی که شامل یک خرابکاری مخرب به گوشی متأثر است از این آسیب‌پذیری سواستفاده کند. یک مهاجم ناشناس راه‌دور می‌تواند باعث شود گوشی متأثر به طور غیرمنتظره‌ای مجدداً بارگذاری شود و منجر به انکار سرویس () شود.

علاوه‌براین، سیسکو ۱۸ نقص با شدت متوسط را نیز در محصولات مختلف خود برطرف ساخته است که می‌تواند برای اسکریپت‌نویسی متقابل ()، حملات جعل درخواست متقابل ()، تزریق فرمان، دورزدن قابلیت فیلترسازی، انکار سرویس یا دسترسی به اطلاعات حساس مورد سواستفاده قرار گیرد.

از جمله این آسیب‌پذیری‌های با شدت متوسط، نقص جعل درخواست متقابل (۱۷۱۳–۲۰۱۹– ،) در رابط مدیریتی مبتنی بر وب در نرم‌افزار)) سیسکو است. این نقص به یک مهاجم راه‌دور احرازهویت‌نشده اجازه می‌دهد تا به لطف حفاظت‌های ناکافی برای واسط مدیریتی مبتنی بر وب ، از سیستم آسیب‌دیده سواستفاده کند. یک مهاجم می‌تواند با متقاعدکردن یک کاربر واسط به دنبال‌کردن یک لینک مخرب، از این آسیب‌پذیری سواستفاده کند.

انتهای پیام/