کد خبر: ۹۹۹۷۸۰
یکشنبه ۲۶ اسفند ۱۳۹۷ ۱۳:۲۴

هشدار مرکز ماهر درباره آسیب‌پذیری بحرانی برخی محصولات سیسکو

مرکز ماهر وزارت ارتباطات درباره آسیب‌پذیری بحرانی برخی محصولات سیسکو هشدار داد.

به گزارش گروه علم و فناوری ایسکانیوز، مرکز ماهر با انتشار اطلاعیه‌ای اعلام کرد: یک آسیب‌پذیری بحرانی در مسیریاب‌های ویژه دفاتر کوچک سیسکو (۱۳۰,۲۱۵ ,۱۱۰) و یک آسیب‌پذیری با درجه اهمیت بالا در محصولات ویدئوکنفرانس سیسکو وجود دارد که منجر به اجرای کد دلخواه می‌شوند. برای این محصولات بروزرسانی امنیتی منتشر شده است.

آسیب‌پذیری در مسیریاب‌های ویژه دفاتر کوچک

یک آسیب‌پذیری بحرانی در رابط تحت وب مسیریاب‌های سیسکو ویژه دفاتر کوچک وجود دارد که امکان اجرای کد دلخواه را توسط مهاجمِ راه دور، بدون نیاز به احراز هویت فراهم می‌کند. این آسیب‌پذیری، ناشی از اعتبارسنجی نامناسب داده‌های ورودی است. مهاجم می‌تواند با ارسال درخواست مخرب از این نقص سواستفاده کند. بهره‌برداری موفق از این آسیب‌پذیری می‌تواند منجر به اجرای کد دلخواه با دسترسی بالا روی سیستم‌عامل تجهیز شود.

این مرکز با معرفی شناسه آسیب‌پذیری (۱۶۶۳-۲۰۱۹-) و درجه اهمیت این آسیب‌پذیری (بحرانی ۹.۸ ۳)، مشخصات تجهیزات آسیب‌پذیر را اینگونه اعلام کرد:

- ۱۱۰

- ۱۳۰

- ۲۱۵

رابط تحت وب این تجهیزات از طریق شبکه محلی () و یا از طریق ویژگی مدیریت راه دور ( ) قابل دسترسی است. البته ویژگی مدیریت راه دور به طور پیش‌فرض غیرفعال است.

براساس اعلام مرکز ماهر، در نسخه‌های نرم‌افزاری زیر، این نقص برطرف شده است. همه نسخه‌های ماقبل، آسیب‌پذیر هستند:

۱.۲.۲.۱ : - ۱۱۰

۱.۰.۳.۴۵ : - ۱۳۰

۱.۳.۱.۱ : – ۲۱۵

آسیب‌پذیری در محصولات ویدئوکنفرانس

آسیب‌پذیری با درجه اهمیت بالا در نرم‌افزار دسکتاپ و نسخه ویندوز وجود دارد. این آسیب‌پذیری به مهاجم محلیِ احراز هویت نشده اجازه می‌دهد دستورات دلخواه را با دسترسی بالا (در چارچوب کاربر) اجرا کند.

هرچند برای بهره‌برداری از این نقص، مهاجم به دسترسی محلی نیاز دارد، اما در محیط‌های دارای ، می‌توان با استفاده از ابزارهای مدیریتی راهِ دور، از این نقص بهره‌برداری کرد.

شناسه: ۱۶۷۴–۲۰۱۹–

درجه اهمیت: بالا ۷.۸ ۳

راه حل موجود برای این آسیب‌پذیری نیز ارتقای نرم‌افزارهای معرفی شده به نسخه به‌روزشده مطابق جدول زیر است.

انتهای پیام/