هشدار آسیب‌پذیری			
موضوع	آسیب‌پذیری اجرای دستور از راه دور رابط مدیریت مسیریاب‌های سیسکو		
شماره هشدار	۱۲	**تاریخ صدور هشدار**	۲۷ تیر ۱۳۹۸
تشریح تهدید	آسیب‌پذیری در رابط مدیریت مبتنی بر وب مسیریاب‌های نسخه RV110W، RV130W و RV215W شرکت سیسکو شناسایی شده است که به مهاجمین تصدیق هویت نشده و از راه دور اجازه می‌دهد کدهای دلخواه بر روی تجهیزات آسیب‌پذیر اجرا کنند. این آسیب‌پذیری به دلیل اعتبارسنجی نادرست اطلاعات وارد شده توسط کاربر به رابط مدیریت وب مسیریاب‌ها رخ می‌دهد که یک مهاجم می‌تواند با ارسال درخواست‌های HTTP مخرب به دستگاه هدف آن را مورد بهره‌برداری قرار بدهد. بهره‌برداری موفق از این آسیب‌پذیری به مهاجم اجازه خواهد داد کدهای دلخواه بر روی سامانه‌عامل دستگاه آسیب‌پذیر با سطح دسترسی بالا اجرا کند. این آسیب‌پذیری به صورت مشخص محصولات زیر را تحت تاثیر قرار می‌دهد: 1. RV110W Wireless-N VPN Firewall 2. RV130W Wireless-N Multifunction VPN Router 3. RV215W Wireless-N VPN Router رابط مدیریت مبتنی بر وب این تجهیزات از طریق ارتباطات محلی و همچنین راه دور قابل دسترس هستند، اگرچه به صورت پیش‌فرض غیرفعال است. برای اینکه اطمینان حاصل کنید که آیا این ویژگی فعال است یا خیر، می‌توانید با رجوع به Basic Settings و سپس Remote Management مطمئن شوید که آیا گزینه Enable تیک خورده است یا خیر. اگر این گزینه تیک خورده باشد، یعنی این ویژگی بر روی دستگاه آسیب‌پذیر شما فعال و در نتیجه دستگاه مستعد حملات سایبری است.		
راه‌حل کاهش تهدید	سیسکو برای این آسیب‌پذیری وصله امنیتی ارائه کرده است. از همین روی، برای رفع آسیب‌پذیری مذکور کافی است، محصولات آسیب پذیر را به آخرین وصله‌های امنیت به روزرسانی کنید.		
شناسه آسیب‌پذیری	CVE-2019-1663	**شدت آسیب‌پذیری**	۹٫۸
منابع	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex		