بسمه تعالی

عنوان خبر:

وصله آسیب‌پذیری روز صفرم SQL Injection و Code Execution در فایروال Sophos

Sophos یک آسیب‌پذیری SQL injection در محصول فایروال XG خود را که توسط مهاجمان در سراسر دنیا مورد اکسپلویت قرار گرفته بود، وصله کرد.

این شرکت در تاریخ ۲۲ آوریل ۲۰۲۰، از این نقص در فایروال خود مطلع گشت و براساس بررسی‌های انجام شده بیان کرد که هکرها می‌توانند سیستم‌هایی با رابط کاربری administration (HTTPS admin service) و یا پورتال کاربری در معرض منطقه WAN را مورد حمله قرار دهند.

همچنین فایروالی که به صورت دستی پیکربندی شده باشد و پورتی مشابه admin یا User Porta را به اشتراک می‌گذارد نیز تحت تاثیر این آسیب‌پذیری قرار می‌گیرد.

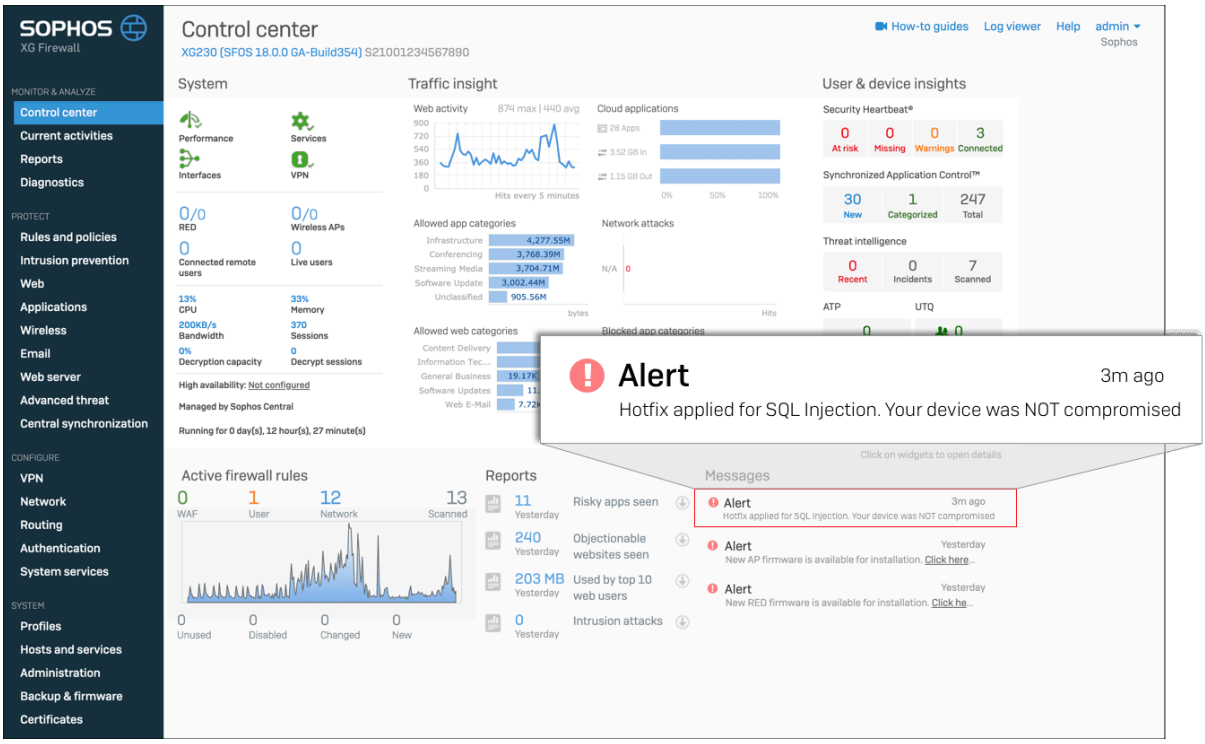
یک مهاجم می‌تواند از آسیب‌پذیری pre-auth SQL injection برای دستیابی به دستگاه‌های فایروال XG، سوء استفاده کرده و با استفاده از این نقص، یک فایل مخرب را بر روی دستگاه بارگیری کند.

مهاجم به کمک این کد مخرب می‌تواند نام‌های کاربری و رمزهای عبور هش شده را از هر حساب کاربری محلی دریافت کند. این حساب‌های کاربری شامل حساب‌های کاربری admin لوکال دستگاه، حساب‌های پورتال کاربر و حساب‌هایی است که برای دسترسی از راه دور یا remote استفاده می‌شوند. رمزهای عبور مرتبط با سیستم‌های احراز هویت خارجی مانند Active Directory (AD) یا LDAP در معرض خطر قرار ندارند.

طبق اظهارات شرکت Sophos، هیچ نشانه‌ای مبنی بر دسترسی مهاجمان به شبکه محلی خارج از دستگاه‌های فایروال XG وجود ندارد. پس از تشخیص مؤلفه‌ها و تاثیر حمله، Sophos یک عیب‌یاب (hotfix) را در تمامی نسخه‌های XG Firewall/SFOS پشتیبانی شده خود، مستقر ساخت.

هدف از این hotfix رفع آسیب‌پذیری SQL injection و جلوگیری از سوء استفاده بیشتر از آن است که فایروال XG را از دسترسی به زیرساخت‌های هر مهاجم متوقف کرده و تمام بقایای حمله را از بین برده است.

به کاربران توصیه می‌شود به منظور رفع این آسیب‌پذیری، hotfix را بر روی دستگاه خود اعمال نمایند و در دستگاه‌های در معرض خطر، رمزهای عبور تمام حساب‌های کاربری محلی مجددا تنظیم و reset شوند.



آسیب‌پذیری مذکور، تمام نسخه‌های Sophos XG Firewall firmware بر روی هر دو فایروال فیزیکی و مجازی را تحت تاثیر قرار می‌دهد. این شرکت hotfix (SFOS 17.0, 17.1, 17.5, 18.0) را نیز در اختیار کاربران قرار می‌دهد. به کاربرانی که از نسخه‌های قدیمی استفاده می‌کنند توصیه می‌شود آن را به جدیدترین نسخه ارتقاء دهند.

منبع خبر:

https://gbhackers.com/sophos-xg-firewall/