

Google Revela Vulnerabilidad De Windows

Investigador de Google [ha descubierto](#) y revelado un error que permite la **escalada de privilegios en Windows**. El investigador de apellido Forshaw se ha contactado con [Microsoft](#) y [Google](#) para hacer comentarios. **Forshaw** incluyó una prueba de concepto del programa ([POC](#)) de la vulnerabilidad. Dice que sólo ha probado en la **versión 8.1 de Windows actualizado** y que aún no está claro si las versiones anteriores, específicamente la de Windows 7, son vulnerables.



La vulnerabilidad se identifica en la **función AhcVerifyAdminContext**. Esto parece ser una función interna y no una API pública, ya que puedes realizar una búsqueda en microsoft.com la cual no te arrojaría alguna información oficial, solo podrás encontrar las relacionadas con el informe de Forshaw.

La prueba de concepto incluye dos archivos de programa y un conjunto de **instrucciones para ejecutar** lo que sería la **calculadora de Windows** que se ejecuta como administrador. Forshaw afirma que el fallo no es en sí en el uso de UAC, pero que UAC se utiliza en parte para demostrar el error.

google-security-research
Google Security Research

Project Home Wiki Issues Source

New issue Search Open issues for Search Advanced search Search tips SI

Issue 118: Windows: Elevation of Privilege in ahcache.sys/NtApphelpCacheControl

Status: Got Token: 000001E4 S-1-5-...
Owner: Interposing on cache for...
Cc: Calling runas on c:\windo...
Vendor: Remove: 00000000
Product: C:\Users\Larry\Downloads\...
Severity: .dll
Finder: Found regsvr32.exe tag: 0...
Reporte: Got Token: 000001E8 S-1-5-...
CCProje: Interposing on cache for...
Deadline: Calling runas on c:\windo...
MSRC-2: Remove: 00000000
Public: C:\Users\Larry\Downloads\...
Deadline: .dll
Add a co: Got Token: 000001E4 S-1-5-...
Interposing on cache for...
Calling runas on c:\windo...
Remove: 00000000
C:\Users\Larry\Downloads\...

Calculator

Command Prompt

RegSvr32

DllRegisterServer in C:\Users\Larry\Downloads\poc\bin\testdll.dll succeeded.

perform the following steps:

- 1) Put the AppCompatCache.exe and Testdll.dll on disk
- 2) Ensure that UAC is enabled, the current user is a split-token admin and the UAC setting is the default (no pr
- 3) Execute AppCompatCache from the command prompt with the command line "AppCompatCache.exe c:\windows\system32\ testdll.dll".
- 4) If successful then the calculator should appear running as an administrator. If it doesn't work first time (a program) re-run the exploit from 3, there seems to be a caching/timing issue sometimes on first run.

Forshaw registró la revelación privada el **30 de septiembre** en **la lista de correo de google-security-investigación**. Al final él indicó «Este error está sujeta a un plazo de divulgación de 90 días. Si transcurren 90 días sin un parche ampliamente disponible, el informe de error se convertirá automáticamente visible para el público.» No hay ninguna indicación de que Microsoft se puso en contacto para resolver esta vulnerabilidad de Windows.