Sign in

WiredPulse / **Invoke-HiveNightmare** Public

Notifications   Fork 16   Star 34

<> Code   Issues   Pull requests 2   Actions   Projects   Security   Insights

main

Go to file   <> Code

Invoke-HiveNightmar...

PoC.gif

README.md

📖 README

Invoke-HiveNightmare

PowerShell-based PoC for CVE-2021-36934, which enables a standard user to be able to retrieve the SAM, Security, and Software Registry hives in Windows 10 version 1809 or newer.

Situation

In specific versions of Windows 10, standard users have read/execute rights to files in [SYSTEMROOT]\System32\Config directory, which is where the Registry hives reside on disk. One can't however, simply navigate to the directory and copy/paste as the hives are loaded and into memory upon system boot and are locked. A

About

PoC for CVE-2021-36934, which enables a standard user to be able to retrieve the SAM, Security, and Software Registry hives in Windows 10 version 1809 or newer

📖 Readme

∿ Activity

☆ 34 stars

👁 2 watching

⑂ 16 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages
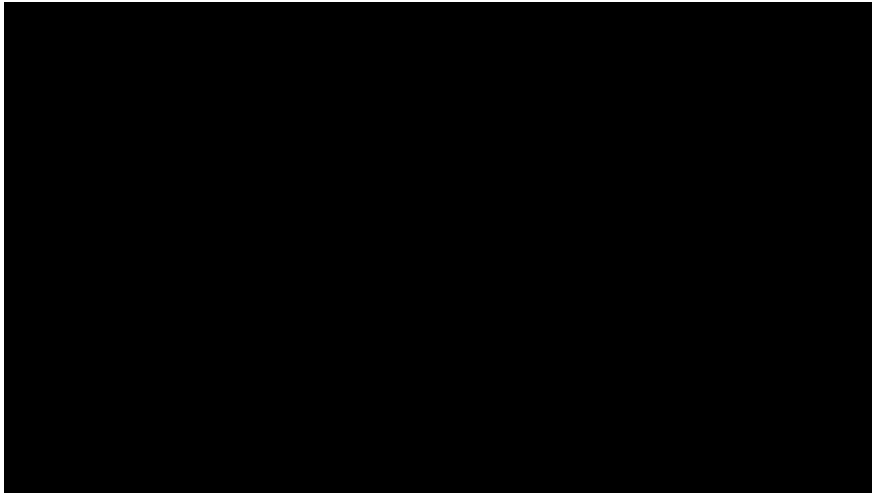
● **PowerShell** 100.0%

standard user can retrieve the hives from Volume Shadow Copies if they exist.

Demo

/ ! [](name-of-gif-file. gif)

Disclaimer

The success of this exploit resides on the fact that Volume Shadows Copies exist... without them the code isn't useful.

Credits

The vulnerability was discovered by @jonasLyk.