Sri Lanka Institute of Information Technology

Windows Privilege SeriousSAM Vulnerability (CVE-2021-36934)

Group Assignment

IE2012 – Systems and Network Programming

Submitted by:

Registration Number	Name
IT21049354	A.M.I.R.B. Athauda
IT21054990	H.M.S.D Herath

Date of Submission
00/00/2022

***Abstract*—This electronic document contains information about a critical vulnerability in the Windows operating system, which has been discovered. In addition to the specifics that are relevant to the users. This document describes the various methods in which a system could be attacked in order to take advantage of this vulnerability. And the effects of this exploitation on the people who have been exploited. The exploitation carried out on two different computers: a Kali Linux machine and a Windows machine. This electronic paper contains information on the procedures to take in order to prevent and reduce these threats.**

I. INTRODUCTION

Jonas Lykkegaard discovered the CVE-2021-36934 vulnerability, also known as SeriousSAM and HiveNightmare, in July 2021. The name 'HiveNightmare' emerges from the common name for files containing registry data, 'hives.' Hives (or hive files) are a shorthand for the proprietary database files that Windows uses to store registry data in the c:\Windows\system32\config folder. Secret data such as passwords and security tokens, which regular users are not supposed to be able to access, are stored in three hive files called SAM, SECURITY, and SYSTEM.

This vulnerability has not been patched by Microsoft until August 10th, 2021. Companies are tried to persuade to implement the most critical mitigations as soon as security patches are made available. Windows 10 version 1809, which was released on October 17th, 2017, and later released windows 10 versions are affected by HiveNightmare. This vulnerability's Proof-of-Concept (POC) exploit code is freely available, but it currently allows for Denial-of-Service (DoS) attacks.

II. LITERATURE SURVEY

On Monday,July 19, 2021, according to community security researchers, Windows 10 and 11 systems' Security Account Manager (SAM) files were made accessible to all local users. A hashed version of each user's and administrator's passwords are stored in the SAM file. In order to escalate their privileges or gain access to additional data in the target environment, attackers need only take root on the system and then use this security-related information. *[1]*

The vulnerability has been confirmed to affect Windows 10 version 1809 and later as of July 22, 2021. Non-admin users can now access all registry hives using a public proof-of-concept. CVE-2021-36934 has been demonstrated in a demo by researcher Kevin Beaumont to allow remote code execution as SYSTEM on arbitrary targets by obtaining local hashes and passing them to a remote machine (in addition to privilege escalation). This vulnerability has been dubbed "HiveNightmare" and "SeriousSAM" by the security community. [1]

In addition, there are a few existing methods of exploitation. The HiveNightmare.exe c++ exploit, this exploit searches for a shadow copy of the system and reads it for SAM, SYSTEM, and SECURITY hives. ' C++ is used to code the exploit. Unlike the HiveNightmare.exe variant, serioussam.psl powershell exploit is written in Powershell, making it more portable than the executable file. After all, the secretsdump.py script from the impacket toolkit will be used to extract the hashes and conduct a pass-the-hash attack after obtaining SAM, SECURITY, and SYSTEM hives. However, system protection must be enabled, and a volume shadow copy must be created for this to be exploit

These are the versions of Windows which were vulnerable to this vulnerability.

- Windows Server, version 20H2 (Server Core Installation)
- Windows Server, version 2004 (Server Core installation)
- Windows Server 2019 (Server Core installation)
- Windows Server 2019
- Windows 10 Version 21H1 for x64-based Systems
- Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 21H1 for 32-bit Systems
- Windows 10 Version 20H2 for x64-based Systems
- Windows 10 Version 20H2 for ARM64-based Systems
- Windows 10 Version 20H2 for 32-bit Systems
- Windows 10 Version 2004 for x64-based Systems
- Windows 10 Version 2004 for ARM64-based Systems
- Windows 10 Version 2004 for 32-bit Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1809 for x64-based Systems
- Windows 10 Version 1809 for ARM64-based Systems
- Windows 10 Version 1809 for 32-bit Systems [2]

As soon as an attacker gains access to a system, this vulnerability allows them to easily accomplish the following:

- Elevate privileges to the administrator level
- Discover the default password for installing Windows
- Obtain the DPAPI computer keys necessary for decrypting the computer's other private keys [3]

The 4.0 patch, released on August 10th, 2021, for this CVE-2021-36934. Since this attack doesn't require any sort of authentication or special access, it becomes incredibly simple for an attacker to affect either the client or the server's final communication.

III. METHODOLOGY

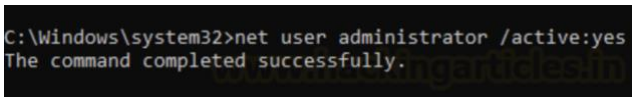
The SeriousSAM or HiveNightmare vulnerability, known as CVE-2021-36934, has been selected for this report. Capturing hashes from the non-privilege account, allowed us to perform a privilege escalation.

We used Google's search engine to do some preliminary research before attempting this exploitation. So, the exploitation works like this.

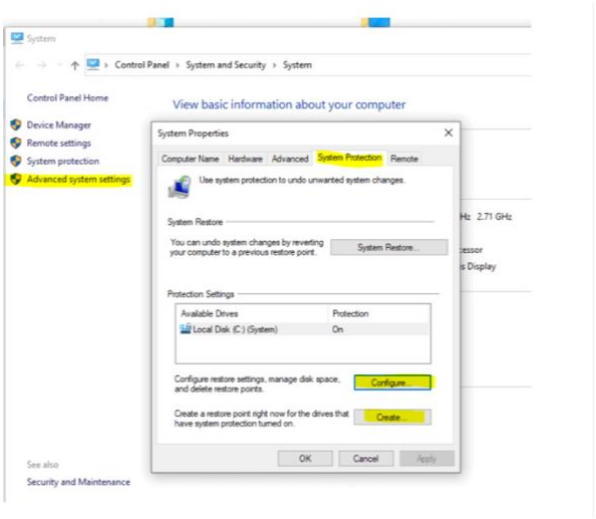
Two computers were used for this exploitation. Kali Linux is running in one virtual machine, while Windows is used in the other. We used Windows 10 Version 2004 64-bit and Kali Linux 2022.1 as the Windows and Kali versions.

The exploitation is as below,

(1) Setting up a lab is the first step in demonstrating this vulnerability's exploitation. After a fresh install of Windows 10, we activated the administrator account. protection.

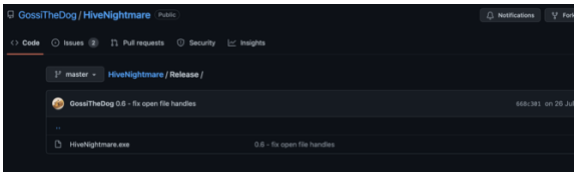


(2) Next, we'll also need to activate system protection. Control Panel > System and Security > System & Security > System Protection > Configure system

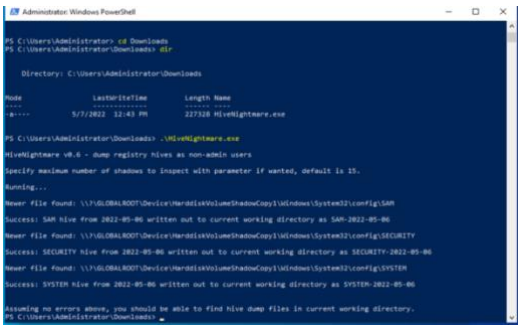


(3) Afterwards, we need to set up our kali environment for the attack. To proceed, we must first install the most recent version of Python on our Kali Linux system because it comes with pre-installed wide range of useful packages. This allows us to use standard libraries such as impacket-secrectsdump and impacket-psexec, which we need for this exploit.

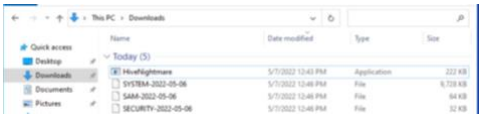
(4) To collect the hashes and other information from the system, we must first download HiveNightmare.exe with a non-administrator account from the GitHub repository. For this, we got it from this git repository.
https://github.com/GossiTheDog/HiveNightmare



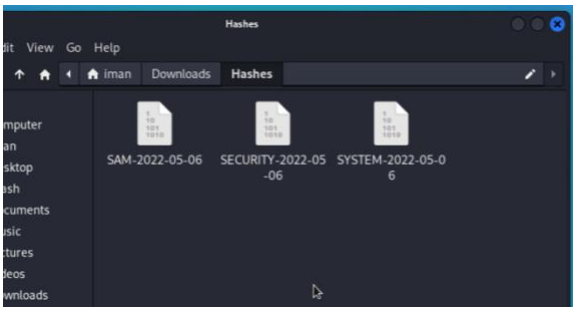
(5) After that, we'll need to use PowerShell to run HiveNightmare.exe and gather all the necessary hashes and system data for the exploit.



Extracted hashes will show as below in the certain directory,

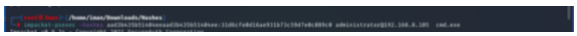


(6) Then we need to copy the extracted SAM, SECURITY, and SYSTEM files into our kali Linux machine.



(7) After files have been copied (SAM, SECURITY, and SYSTEM), we need to dump the hashes from them. For that we are using impacket-secrets dump command as in the screenshot. Python script Secretsdump can be used to extract NTLM password hashes from a variety of file types. In the end of the command, we used 'local' to tell it just use these local files that we are providing.

(8) As soon as we have all the hashes, we need to perform an exploit to gain administrator privileges. In order to perform the exploit, type the following command. The psexec.py script is one of the incredibly valuable penetration testing scripts included with the IMPACKET Python package.



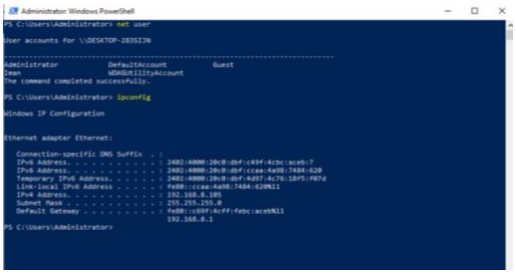
We'll be able to run cmd.exe as the administrator after entering these commands. To access the Administrator account, we must enter the dumped hash, as well as the administrator's name, IP address, and cmd.exe.

The Administrator's privileges have now been elevated.

IV. RESULTS AND MITIGATION

IV.I RESULTS

This cve-2021-3634 exploitation, as well as the one above, demonstrates just how critical it was. The administrator's privileges can be elevated by capturing the machine's hash and u sing the IP address. Because this exploit can be carried out at any level of authority, we have a high success rate in exploiting it. In addition, we are allowed to read, write, and execute. Moreover, we can control the machine as our desire.



We'll have access to everything in the system files if we're successful in exploiting it. An example of this can be seen in the picture below.

IV.II MITIGATION

This vulnerability poses a serious risk to any organization because of how easily it can be exploited. As a result, Microsoft has made security patches available. It is well-known that no system is completely secure. There are and will be ways for an attacker to exploit these vulnerabilities in systems. As a result of this vulnerability's criticality, all servers and workstations that share it should have alternative solutions implemented to prevent its exploitation. To prevent from this vulnerability following workarounds are suggested.

(1)Restrict access to the contents of %windir%\system32\config

- *Command Prompt (Run as administrator):*

icacls %windir%\system32\config*.* /inheritance:e

- *Windows PowerShell (Run as administrator):*

icacls $env:windir\system32\config*.* /inheritance:e [4]

(2) Delete Volume Shadow Copy Service (VSS) shadow copies

- *Command Prompt or PowerShell can be used to determine if there are any shadow volumes (Run as administrator):*
  vssadmin list shadows

- *Remove any System Restore points and Shadow Volumes that were created before restricting access to* %windir%\system32\config [4]

V. CONCLUSION

An attacker who was able to take advantage of this vulnerability would be able to execute code with the super-high SYSTEM privileges. Full user access means that they can install programs; alter or delete data; or create new accounts with full user rights. As a result, we must safeguard our systems by performing an automatic update as soon as a new version is available. Keeping up with the latest cyber-world news is another way to keep yourself safe.

REFERENCES

[1] "https://www.rapid7.com/blog/post/2021/07/21/microsoft-sam-file-readability-cve-2021-36934-what-you-need-to-know/," [Online].

[2] "https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934," [Online].

[3] "https://medium.com/attivotechblogs/serioussam-aka-hivenightmare-vulnerability-local-privilege-escalation-on-windows-10-2289fb81c933," [Online].

[4] "https://news.sophos.com/en-us/2021/07/22/hivenightmare-aka-serioussam-vulnerability-what-to-do/," [Online].