Microsoft SAM File Readability CVE-2021-36934: What You Need to Know

On Monday, July 19, 2021, community security researchers began reporting that the Security Account Manager (SAM) file on Windows 10 and 11 systems was READ-enabled for all local users. The SAM file is used to store sensitive security information, such as hashed user and admin passwords. READ enablement means attackers with a foothold on the system can use this security-related information to escalate privileges or access other data in the target environment.

On Tuesday, July 20, Microsoft issued an out-of-band advisory for this vulnerability, which is now tracked as CVE-2021-36934. As of July 22, 2021, the vulnerability has been confirmed to affect Windows 10 version 1809 and later, as well as Windows Server 2019 and later. A public proof-of-concept is available that allows non-admin users to retrieve all registry hives. Researcher Kevin Beaumont has also released a demo that confirms CVE-2021-36934 can be used to obtain local hashes and pass them to a remote machine, achieving remote code execution as SYSTEM on arbitrary targets (in addition to privilege escalation). The security community has christened this vulnerability “HiveNightmare” and “SeriousSAM.”

CERT/CC published in-depth vulnerability notes on CVE-2021-36934, which we highly recommend reading. Their analysis reveals that starting with Windows 10 build 1809, the BUILTIN\Users group is given RX permissions to files in the %windir%\system32\config directory. If a VSS shadow copy of the system drive is available, a non-privileged user may leverage access to these files to:

Extract and leverage account password hashes.

Discover the original Windows installation password.

Obtain DPAPI computer keys, which can be used to decrypt all computer private keys.

Obtain a computer machine account, which can be used in a silver ticket attack.

Recommendation:

There is no patch for CVE-2021-36934 as of July 21, 2021. Microsoft has released workarounds for Windows 10 and 11 customers that mitigate the risk of immediate exploitation—we have reproduced these workarounds in the Mitigation Guidance section below. Please note that Windows customers must BOTH restrict access and delete shadow copies to prevent exploitation of CVE-2021-36934. We recommend applying the workarounds on an emergency basis.

Mitigation Guidance

1. Restrict access to the contents of %windir%\system32\config:

- Open Command Prompt or Windows PowerShell as an administrator.
- Run this command:

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

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

Delete any System Restore points and Shadow volumes that existed prior to restricting access to %windir%\system32\config.

Create a new System Restore point if desired.

Windows 10 and 11 users must apply both workarounds to mitigate the risk of exploitation. Microsoft has noted that deleting shadow copies may impact restore operations, including the ability to restore data with third-party backup applications.

References:

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

https://vulners.com/rapid7blog/RAPID7BLOG:21FF66FD08C23AC39BCCB8CFE2238507

Microsoft SAM File Readability CVE-2021-36934: What You Need to Know: SoylentNews Submission