CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-038

Windows Elevation of Privilege Vulnerability

July 23, 2021 — v1.1

TLP:WHITE

History:

- *22/07/2021 — v1.0 – Initial publication*
- *23/07/2021 — v1.1 – Expand affected versions*

Summary

An elevation of privilege vulnerability exists in Windows because of overly permissive Access Control Lists (ACLs) on multiple system files, including the Security Accounts Manager (SAM) database. An attacker who successfully exploited this vulnerability could do privilege escalation and run arbitrary code with SYSTEM privileges [1].

Technical Details

Vulnerability dubbed *HiveNightmare* and *SeriousSAM* has also received CVE-2021-36934. By incorrectly setting Access Control List `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 achieve a number of impacts, including but not limited 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

Affected Products

Windows 10, Windows 11, Windows Server 2019 and Windows Server Coreve versions. For more specific type and version please check [1].

Recommendations

There is no patch for CVE-2021-36934 as of July 21, 2021. It is recommened to apply the workaround available.

Workaround

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`

Delete Volume Shadow Copy Service (VSS) Shadow Copies

1. Delete any System Restore points and Shadow volumes that existed prior to restricting access to `%windir%\system32\config`.
2. Create a new System Restore point (if desired).

Impact of deleting shadow copies could impact restore operations, including the ability to restore data with third-party backup applications. For more information on how to delete shadow copies, see [4].

Note: You must restrict access and delete shadow copies to prevent exploitation of this vulnerability [1].

Exploitation

Exploits are already available for this flaw [3].

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

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

[3] https://github.com/GossiTheDog/HiveNightmare

[4] https://support.microsoft.com/en-us/topic/kb5005357-delete-volume-shadow-copies-1ceaa637-aaa3-4b58-a48b-baf72a2fa9e7