VULNERABILITY BULLETINS

New Windows 10 Elevation of Privilege Vulnerability Discovered

TLP:WHITE

Jul 22, 2021

A new Windows 10 and 11 local elevation of privilege vulnerability has been discovered that enables users with low privileges to access sensitive Registry database files.

An attacker who successfully exploited this vulnerability, designated CVE-2021-36934, could run arbitrary code with full SYSTEM privileges. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights. The attacker must have already gained the ability to execute code on the target system in order to exploit the flaw.

Microsoft has released workarounds and additional mitigations strategies to mitigate this new vulnerability, which can be accessed in this alert.

The Windows Registry acts as the configuration repository for the Windows operating system and contains hashed passwords, user customizations, configuration options for applications, system decryption keys, and more. The database files associated with the Windows Registry are stored under the C[:]\Windows\system32\config folder and are broken up into different files.

As these files contain sensitive information about all user accounts on a device and security tokens used by Windows features, they should be restricted from being viewed by regular users with no elevated privileges. This is also true for the Security Account Manager (SAM) file, as it contains hashed passwords for all users on a system, which a threat actor can use to assume their identity.

Security researchers discovered that the Windows 10 and Windows 11 Registry files associated with the Security Account Manager (SAM), and all other Registry databases, are currently accessible to the Users group that has low privileges on a device. These low permissions were confirmed by researchers on a fully patched Windows 10 20H2 device. With these low file permissions, along with shadow volume copies of the files, a threat actor with limited privileges on a device can extract the NTLM hashed passwords for all accounts on a device and use those hashes in pass-the-hash attacks to gain elevated privileges.

Reference(s)	Bleeping Computer, Malwarebytes Labs, Microsoft, Microsoft

CVE(s)
CVE-2021-36934

Recommendations

Workarounds:

- Restrict access to the contents of %windir%\system32\config, either via Command Prompt or Windows PowerShell.
    - Open Command Prompt as an administrator:
        - Run the following command: icacls %windir%\system32\config*.* /inheritance:e
    - Open Windows PowerShell as a administrator:
        - Run the following command: icacls $env:windir\system32\config*.* /inheritance:e
- 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).
- Impact of workaround:
    - Deleting shadow copies could impact restore operations, including the ability to restore data with third-party backup applications.

Additional info on how to delete shadow copies is available in the Microsoft KB5005357- Delete Volume Shadow Copies support document.

Sources
Microsoft: Windows Elevation of Privilege Vulnerability

Bleeping Computer: New Windows 10 Vulnerability Allows Anyone to Get Admin Privileges

Malware Bytes: HiveNightmare zero-day lets anyone be SYSTEM on Windows 10 and 11

KB5005357- Delete Volume Shadow Copies

Alert ID 7d560b05

View Alert

Tags Windows 11, Registry Database, Elevation of privilege vulnerability, Windows 10 Vulnerability, SYSTEM

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**