Windows Elevation Vulnerability – CVE-2021-36934

Microsoft released new vulnerability for Win 10 machines that can be exploited by hackers. Below are the details - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

Executive Summary

An elevation of privilege vulnerability exists 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 run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

An attacker must have the ability to execute code on a victim system to exploit this vulnerability.

Workarounds

Restrict access to the contents of %windir%\system32\config

1. Open Command Prompt or Windows PowerShell as an administrator.
2. Run this command: `icacls %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 workaround Deleting shadow copies could impact restore operations, including the ability to restore data with third-party backup applications.

Note You must restrict access *and* delete shadow copies to prevent exploitation of this vulnerability.

No versions of Windows are listed in the Security Updates table. Are all versions vulnerable?

So far, we can confirm that this issue affects Windows 10 version 1809 and newer operating systems. We will update this CVE as we continue our investigation. If you wish to be notified when updates are released, we recommend that you register for the security notifications mailer to be alerted of content changes to this CVE. See Microsoft Technical Security Notifications.

Thanks

Ram Lan
21st Jul 2021