How to fix errors for ACL and SAM vulnerabilities on Windows

Microsoft Security has been talking about a relatively new system vulnerability for the past few days called ACL & SAM, and the company is rolling out a fix guide.

The recently discovered CVE-2021-36934 vulnerability is an important issue because it provides elevated privileges to the bad guys.

The elevated privilege vulnerability exists because Access Control Lists (ACLs) are too permissive on many system files, including the Security Accounts Manager (SAM) database. An attacker who successfully exploited this vulnerability could run arbitrary code with system privileges. They can then install programs, view, change or delete data; or create a new account with full user rights.

To exploit the vulnerability, the bad guys must have access to the system and run the code in the first place. Microsoft is still investigating the issue and more data is expected to be added to the CVE. However, for now, users can try 2 methods to disable the vulnerable part of the operating system.

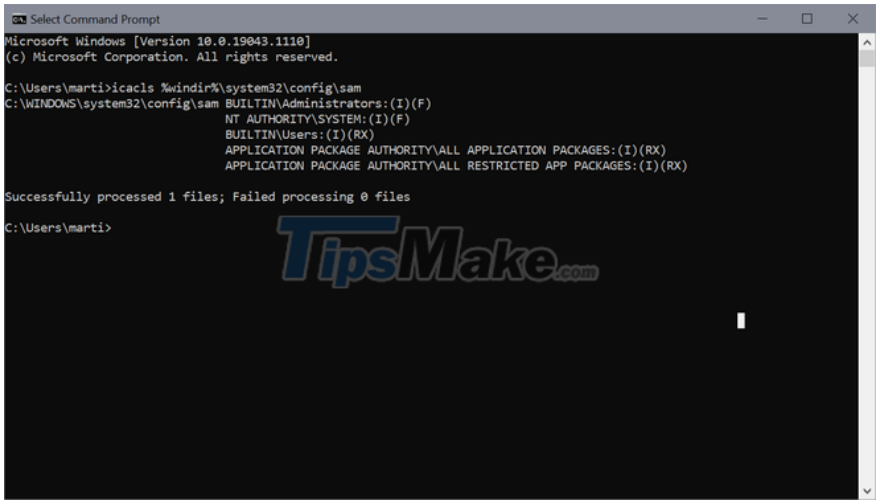
According to the official version, no vulnerabilities were exploited and Microsoft was quick enough to come up with an alternative. However, the company also mentioned that exploits using the vulnerability are more likely to happen and users must follow the workaround as quickly as possible.

How to fix

First, you have to run Command Prompt or Windows PowerShell command execution application and run below command to limit access to %windir%system32config folder.

With Command Prompt: icacls %windir%system32config*.* /inheritance:e

With PowerShell: icacls $env:windirsystem32config*.* /inheritance:e



In the second step, the user must delete the copy of the Volume Shadow Copy Service. And will also require deleting System Restore's restore points.

Once they have been removed and access to the %windir%system32config folder is restricted, the user can create another System Restore point.

The problem with the workaround is that the user will lose access to existing System Restores. That won't be a problem for those with another form of backup, but individuals or organizations that rely entirely on System Restore points will be at risk.

It should be noted that the current workaround is a temporary workaround. Microsoft will likely release a patch after thoroughly investigating the issue.

You finished reading the article "**How to fix errors for ACL and SAM vulnerabilities on Windows**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.