Report

Archived: 2026-04-05 20:34:32 UTC

-- **(Type-Attack A)** The first one is to create the Registry Key `"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\MiniNt"`. This action will not generate Security EventLog 4657 or Sysmon EventLog 13 because the value of the key remains empty. However, if an attacker uses powershell to perform this attack (and not cmd), a Security EventLog 4663 will be generated (but 4663 generates a lot of noise).

-- **(Type-Attack B)** The second way is to disable the service EventLog (display name Windows Event Log). After disabed, attacker must reboot the system. The action of disabling or put in manual the service will modify the Registry Key value `"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\start"`, therefore Security EventLog 4657 or Sysmon EventLog 13 will be generated on the system.

-- **(Type-Attack C)** The third way is linked with the second. By default, the EventLog service cannot be stopped. If an attacker tries to stop the service, this one will restart immediately. Why ? Because to stop completely, this service must stop others, one in particular called netprofm (display name Network List Service). This service remains running until it is disabled. So Attacker must either disable EventLog and after to stop it or disable netprofm and after stop EventLog. Only stopping the service (even as admin) will not have an effect on the EventLog service because of the link with netprofm. Security EventLog 1100 will log the stop of the EventLog service (but also generates a lot of noise because it will generate a log everytime the system shutdown). We can stop the service (with Stop-Service) only if we disable it with the commands Set-Service or sc config. Direct modification of the registry key using reg add, New-ItemProperty, Set-ItemProperty will disable the service only after system restart.

-- **(Type-Attack D)** The fourth way is to use auditpol.exe to modify the audit configuration and disable/modify important parameters that will lead to disable the creation of EventLog.

-- **(Type-Attack E)** The fifth way is to modify the Registry Key value `"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security\file"` (or other kind of log) to modify the path where the EventLog are stocked. Importantly, with this technique, the EventViewer will use the value of the Registry Key `"file"` to know where to find the Log. Thus, using the EventViewer will always show the current event logs, but the old one will be stocked in another evtx. Also, the location of the file must be writable by the Event Log service and should only be accessible to administrators. Attacker can also decrease the maxsize value of the Log to force the system to rewrite on the older EventLog (but the minimum cannot be less than 1028 KB). As the Registry key is modified, Security EventLog 4657 or Sysmon EventLog 13 will be generated on the system. All of these attacks required administrative right. Attacks number three, four and five do not require a system reboot to be effective immediately.

-- **(Type-Attack F)** Fixed in Windows 11 version One discovered during my LAB is a new way to disable Security EventLog without needing the administrator privilege (tested on Microsoft Windows [Version 10.0.17763.1935]). A non-admin user can modify the `"start"` value in the registry

`"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Security"` to completely disable the Security EventLog. However the system reboot is required to take effect. After the reboot, a System Eventlog 22 is generated and the Security EventLog will be Completely Unavailable. Adversaries may also modified the `"start"` value in the registry `"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-System"` and `"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Application"` to disable all the EventLog and will be Partially Unavailable. Administrator privilege required. Adversaries may also modify the `"enabled"` values in `"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational\{5770385f-c22a-43e0-bf4c-06f5698ffbd9}"` or value `"start"` in `"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational"` and Sysmon EventLog will be Completely Unavailable. Administrator privilege required.

-- **(Type-Attack G)** Attacker may use the powershell command `"Remove-EventLog -LogName Security"` to unregister source of events that are part of Windows (Application, Security…). This command deletes the security EventLog (which also generates EventId 1102) but the new Eventlogs are still recorded until the system is rebooted . After the System is rebooted, the Security log is unregistered and doesn't log any new Eventlog. However logs generated between the command and the reboot are still available in the .evtx file (Partially Unavailable). This command disables Logs (reboot required) AND deletes EventLogs (reboot NOT required). Attack also present in REP-26-D

Note: We can define the result of the logs availability in 3 categories:
- Completely Unavailable (lost after the configuration revert)
- Partially Unavailable (available after the configuration revert (if log rewriting not done))
- Available in Other File (available in other location)
