Impair Defenses: Disable Windows Event Logging, Sub-technique T1562.002 - Enterprise

Archived: 2026-04-05 15:36:14 UTC

Adversaries may disable Windows event logging to limit data that can be leveraged for detections and audits. Windows event logs record user and system activity such as login attempts, process creation, and much more.[1] This data is used by security tools and analysts to generate detections.

The EventLog service maintains event logs from various system components and applications.[2] By default, the service automatically starts when a system powers on. An audit policy, maintained by the Local Security Policy (secpol.msc), defines which system events the EventLog service logs. Security audit policy settings can be changed by running secpol.msc, then navigating to `Security Settings\Local Policies\Audit Policy` for basic audit policy settings or `Security Settings\Advanced Audit Policy Configuration` for advanced audit policy settings.[3][4] `auditpol.exe` may also be used to set audit policies.[5]

Adversaries may target system-wide logging or just that of a particular application. For example, the Windows EventLog service may be disabled using the `Set-Service -Name EventLog -Status Stopped` or `sc config eventlog start=disabled` commands (followed by manually stopping the service using `Stop-Service -Name EventLog`).[6][7] Additionally, the service may be disabled by modifying the "Start" value in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog` then restarting the system for the change to take effect.[7]

There are several ways to disable the EventLog service via registry key modification. First, without Administrator privileges, adversaries may modify the "Start" value in the key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Security`, then reboot the system to disable the Security EventLog.[8] Second, with Administrator privilege, adversaries may modify the same values in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-System` and `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Application` to disable the entire EventLog.[7]

Additionally, adversaries may use `auditpol` and its sub-commands in a command prompt to disable auditing or clear the audit policy. To enable or disable a specified setting or audit category, adversaries may use the `/success` or `/failure` parameters. For example, `auditpol /set /category:"Account Logon" /success:disable /failure:disable` turns off auditing for the Account Logon category.[9][10] To clear the audit policy, adversaries may run the following lines: `auditpol /clear /y` or `auditpol /remove /allusers`.[10]

By disabling Windows event logging, adversaries can operate while leaving less evidence of a compromise behind.

Source: https://attack.mitre.org/techniques/T1562/002