Microsoft Defender Exploit Guard audit events for Vision Pro

Article Number: 537 | Last Updated: Tue, Mar 23, 2021 11:47 AM

Block credential stealing from the Windows local security authority subsystem There are three processes that generate 1121/1122 messages in Defender events: Â Â Microsoft Defender Exploit Guard has blocked an operation that is not allowed by your IT administrator.   Â Â For more information please contact your IT administrator.   Â Â ID: 9E6C4E1F-7D60-472F-BA1A-A39EF669E4B2   Â Â User: NT AUTHORITY\SYSTEM   Â Â **Path**: C:\Windows\System32\lsass.exe   Â Â **Process Name**: C:\Program Files (x86)\Netop\Vision\XL\MeSuAx.exe C:\Program Files (x86)\Netop\Vision\XL\MeCfgVrf.exe C:\Program Files (x86)\Netop\Vision\XL\mesuwts.exeÂ Â   None of the above applications are trying to steal credentials. Instead, they are procedures that verify if different Vision applications are running, by searching in the active processes page. For enumerating processes, there are two methods used in these applications: **EnumProcesses(...)** and **WTSEnumerateProcesses(...)**, both of them generating the exception messages from above: "In some apps, the code enumerates all running processes and attempts to open them with exhaustive permissions. This rule denies the app's process open action and logs the details to the security event log. This rule can generate a lot of noise. If you have an app that simply enumerates LSASS, but has no real impact in functionality, there is NO need to add it to the exclusion list. By itself, this event log entry doesn't necessarily indicate a malicious threat." For more information about the Microsoft Defender security messages and audit events, refer to the following Microsoft article.Â

Posted - Tue, Mar 23, 2021 11:07 AM.

Online URL:
https://kb.netop.com/article/microsoft-defender-exploit-guard-audit-events-for-vision-pro-537.html