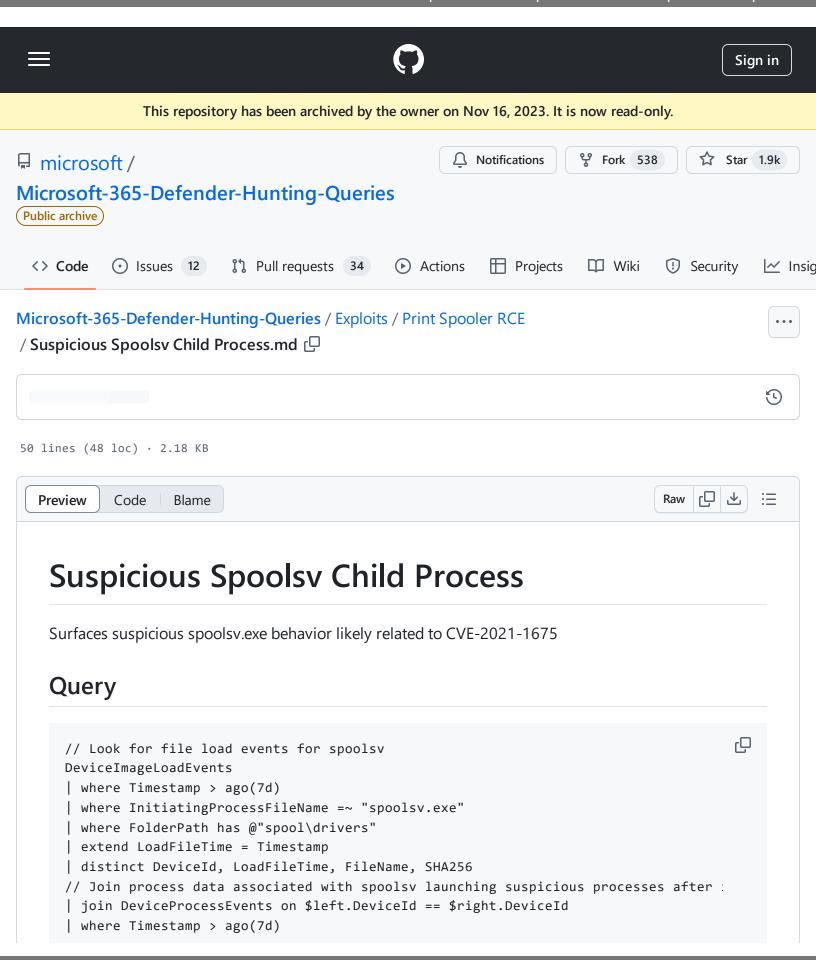
Microsoft-365-Defender-Hunting-Queries/Exploits/Print Spooler RCE/Suspicious Spoolsv Child Process.md at efa17a600b43c897b4b7463cc8541daa1987eeb4 · microsoft/Microsoft-365-Defender-Hunting-Queries · GitHub - 31/10/2024 19:18 https://github.com/microsoft/Microsoft-365-Defender-Hunting-

Queries/blob/efa17a600b43c897b4b7463cc8541daa1987eeb4/Exploits/Print%20Spooler%20RCE/Suspicious%20Spoolsv%2



Microsoft-365-Defender-Hunting-Queries/Exploits/Print Spooler RCE/Suspicious Spoolsv Child Process.md at efa17a600b43c897b4b7463cc8541daa1987eeb4 · microsoft/Microsoft-365-Defender-Hunting-Queries · GitHub - 31/10/2024 19:18 https://github.com/microsoft/Microsoft-365-Defender-Hunting-

Queries/blob/efa17a600b43c897b4b7463cc8541daa1987eeb4/Exploits/Print%20Spooler%20RCE/Suspicious%20Spoolsv%2

Category

This query can be used to detect the following attack techniques and tactics (<u>see MITRE ATT&CK</u> framework) or security configuration states.

Technique, tactic, or state	Covered? (v=yes)	Notes
Initial access		
Execution		
Persistence		
Privilege escalation	V	
Defense evasion		
Credential Access		
Discovery		
Lateral movement		
Collection		
Command and control		
Exfiltration		
Impact		
Vulnerability		

Microsoft-365-Defender-Hunting-Queries/Exploits/Print Spooler RCE/Suspicious Spoolsv Child Process.md at efa17a600b43c897b4b7463cc8541daa1987eeb4 · microsoft/Microsoft-365-Defender-Hunting-Queries · GitHub -31/10/2024 19:18 https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/efa17a600b43c897b4b7463cc8541daa1987eeb4/Exploits/Print%20Spooler%20RCE/Suspicious%20Spoolsv%2