Print spooler vulnerability assessment

You might need to assess your exposure to print spooler vulnerabilities when doing the following:

- Detecting print spooler attacks

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Technologies:
  - Splunk Enterprise or Splunk Cloud Platform
  - Splunk Add-On for Windows
- Data:
  - Windows event logs
  - Microsoft Sysmon

Example

Some attacks such as PrintNightmare use the print spooler to execute code in the target system with the aim of gaining escalated privileges.

As part of a process of detecting attacks on print spooler services in your network, you should first understand your exposure to this vulnerability. You can do this by using Splunk to assess how many endpoints in your network have the print spooler service enabled or running.

To optimize the search shown below, you should specify an index and a time range.

1. Enable Universal Forwarders across your fleet.
2. Enable the WinHostMon input from the Splunk Add-On for Windows to report on the status of services on each server:

```
####### Host monitoring #######
[WinHostMon://Service]
interval = 600
disabled = 0
type = Service
```

3. Run the following search:
source=service DisplayName="Print Spooler" | stats values(DisplayName) AS Disp_Name,values(StartMode) AS Start_mode,values(Started) AS Started,values(State) AS State BY host

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>source=service DisplayName=&quot;Print Spooler&quot;</td>
<td>Search WinHostMon for the Print Spooler service.</td>
</tr>
<tr>
<td></td>
<td>stats values(DisplayName) AS Disp_Name,values(StartMode) AS Start_mode,values(Started) AS Started,values(State) AS State BY host</td>
</tr>
</tbody>
</table>

Result

The results of this search can be used to track mitigation progress. Once you understand your exposure to this vulnerability, you can run additional searches to detect instances where print spooler attacks have occurred.