Detecting print spooler attacks

Scenario: As a security analyst, it is your job to stay on top of Microsoft’s reports on common vulnerabilities and exposures. You have recently found out that Microsoft has reported on a number of vulnerabilities that may affect your network, and you need to identify whether any of your organization’s Windows endpoints have been affected.

These vulnerabilities affect the print spooler service, which is enabled by default on Windows systems, and allows adversaries to trick this service into installing a remotely hosted print driver using a low privileged user account. Successful exploitation allows attackers to execute remote code in the target system in the context of the print spooler service, which then runs with escalated privileges. The PrintNightmare vulnerability is an example of this type of attack.

You can use Splunk software to investigate programs or binaries that executed on the infected system, examine connections the infected machine had to other network devices, construct a timeline of events, and create traffic flow diagrams to help visualize what happened.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Threat hunter, security analyst
- Technologies:
  - Splunk Enterprise or Splunk Cloud Platform
  - Splunk Add-On for Windows
- Data:
  - Windows event logs
  - Microsoft Sysmon

How to use Splunk software for this use case

You can run an initial check to understand your exposure to this type of vulnerability:

- Print spooler vulnerability assessment

To check further for suspicious activity relating to this vulnerability, depending on your environment and requirements, you might find it useful to run some or all of the following:

- Spoolsv spawning Rundll32
- Spoolsv suspicious process access
- Spoolsv suspicious loaded modules
• Spoolsv.exe writing a DLL
• Print spooler adding a printer driver
• Print spooler failing to load a plug-in

Results

During triage, isolate the endpoint and review for source of exploitation. Capture any additional file modification events.

If your results indicate an attack has occurred, the host or computer where the vulnerability is detected needs to be further investigated and remediated according to your response plan. This involves a final step of re-imaging the system with a known good system build after investigation.

Additional resources

The content in this guide comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. In addition, these Splunk resources might help you understand and implement this use case:

• .Conf Talk: Develop endpoint detection superpowers with Sysmon + Splunk