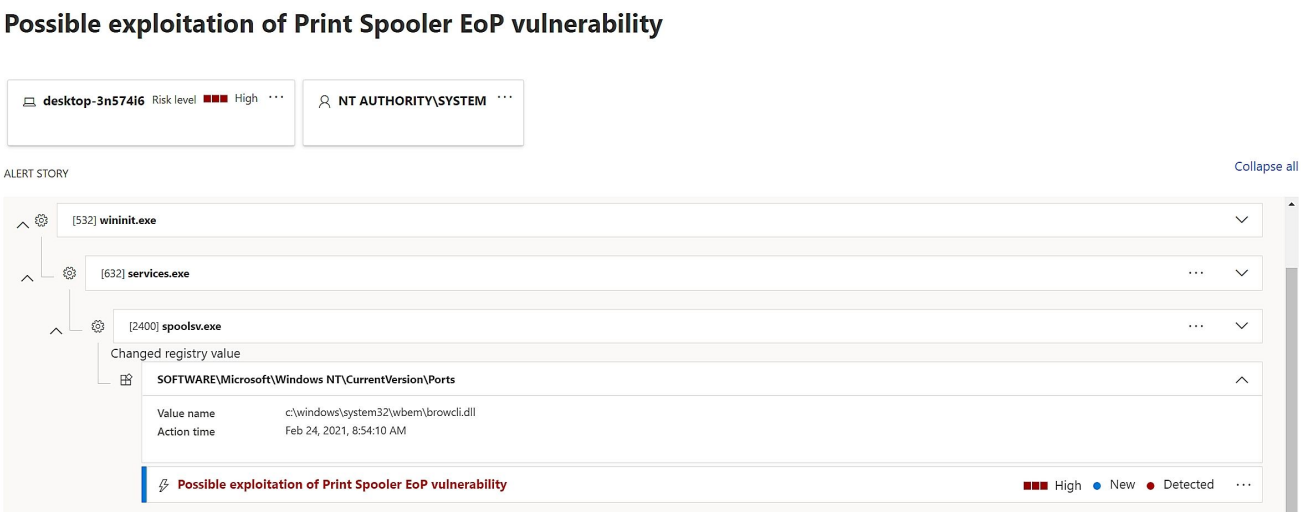
Investigating the Print Spooler EoP exploitation

techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/investigating-the-print-spooler-eop-exploitation/ba-p/2166463

March 8, 2021



We are excited to share a short attack simulation to highlight how Microsoft Defender for Endpoint can alert analysts for every suspicious system event that's related to an intrusion and how analysts can mitigate the attacker's actions right from the alert page. We've chosen a relatively straightforward exploitation scenario which we believe still carries significant risk for organizations that have not been able to update their operating systems. In this scenario, we use the updated Microsoft Defender for Endpoint alert page, which has features to make the investigation experience better and more effective.

SafeBreach, one of our evaluation lab partners for breach and attack simulation solutions, discovered an elevation of privilege vulnerability in the Windows print spooler mechanism. This vulnerability, assigned CVE-2020-1048[i], has already been patched. However, it remains an

interesting case study because of the prevalence of the print spooler mechanism, and the vulnerability's involvement in a widely covered high-profile attack in the past.

The actual exploitation details have already been discussed extensively in other blogs, but in summary, this vulnerability allows an unprivileged user to modify a file that they should not have been able to access, or to create a file in a folder they should not have write access to.

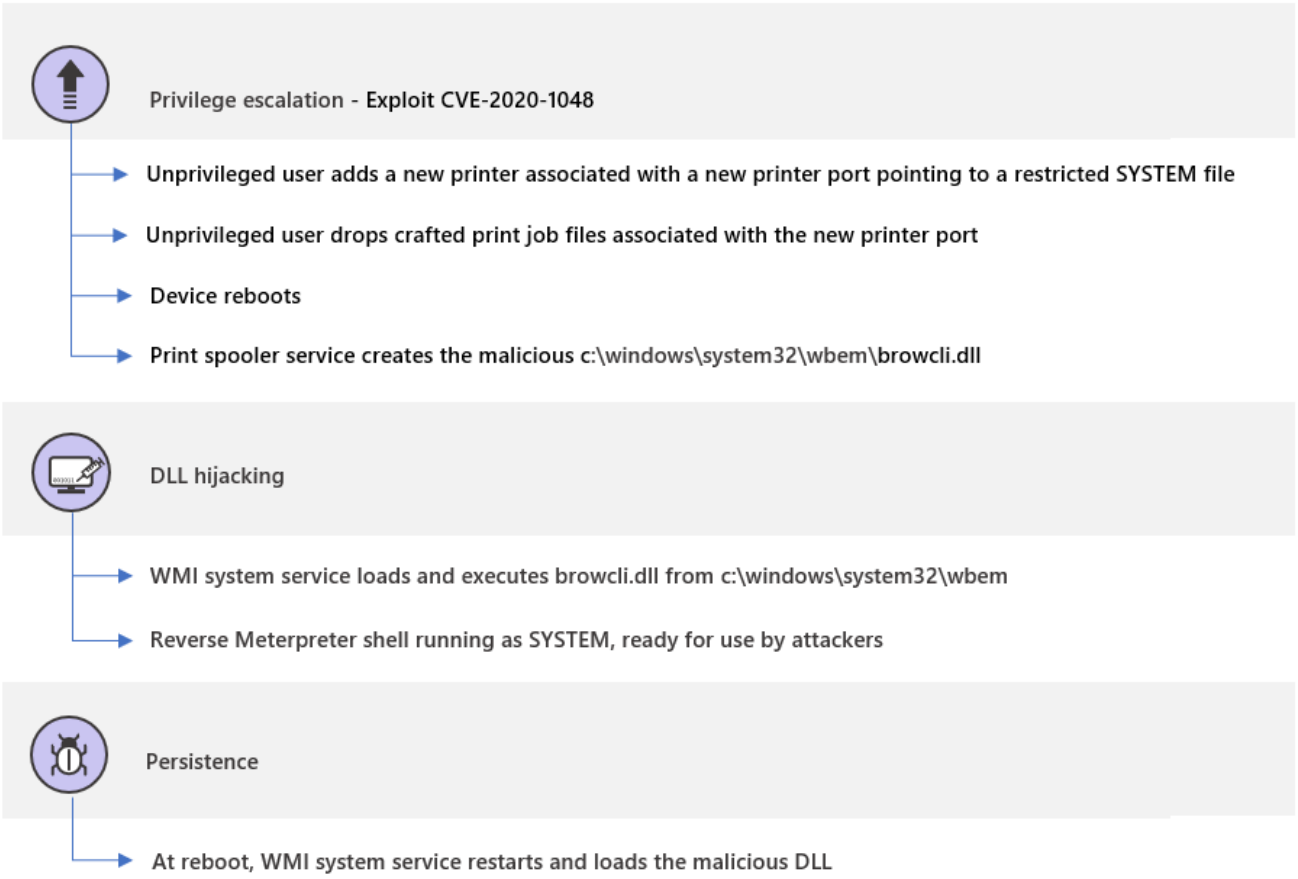


Figure 1. Attack phases of a sample attack using CVE-2020-1048

The print spooler is a Windows component that manages the printing process and runs with system privileges. Specifically, it can write or modify files in the System32 folder. Since this is a common service that comes preinstalled, any suspicious activity initiated by the spooler might be easily missed.

Unprivileged users could easily add new printers in Windows. Every printer is then associated to a port. The catch is that the printer port, instead of being an actual port, could instead be a path to a file. When the port is a file path, the printer creates a file on the file system and prints content to it. Before the vulnerability was patched, this means that any user could print to folders they don't have access to.

Malicious actors can thus use this vulnerability to create a malicious DLL, for instance, print it to the system folder, and wait for the system to run it in a classic DLL hijacking attack. We will use this scenario in our simulation.

Microsoft Defender for Endpoint blocks, detects, and remediates the attack. This blog will cover the phases of the attack and how Defender for Endpoint correlates these to a single view of an incident, providing the full context of the related alerts, impacted entities, and the investigation.

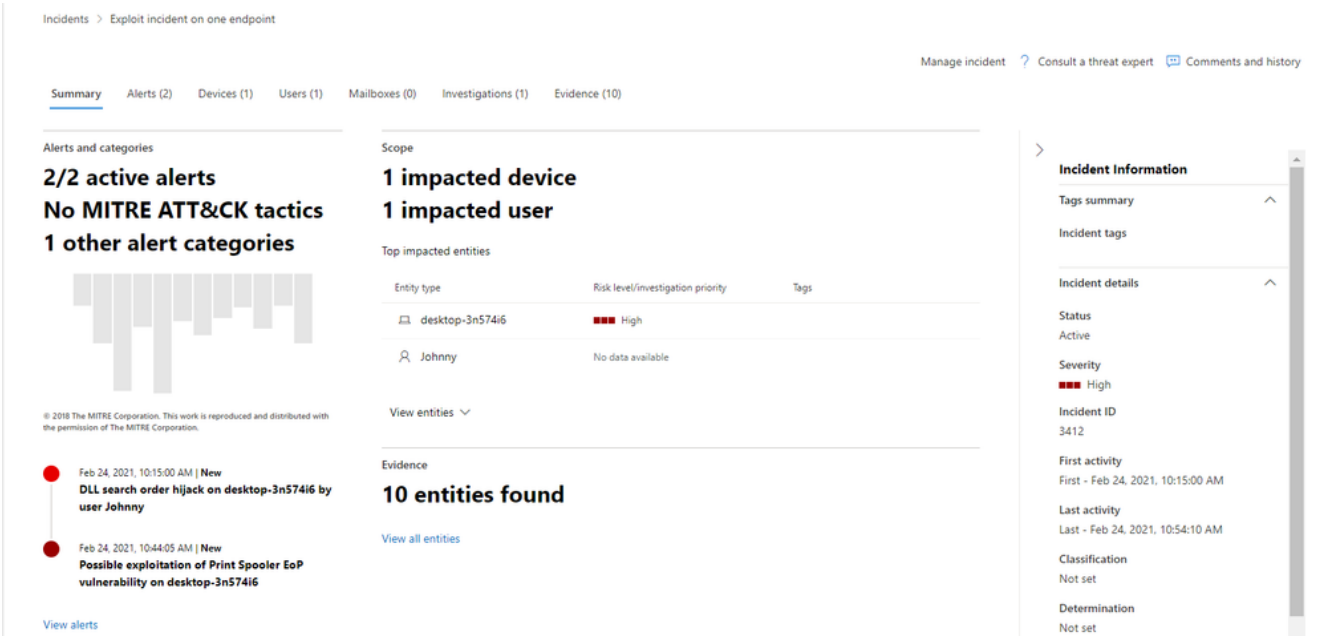


Figure 2. The incident page providing the full context of the attack

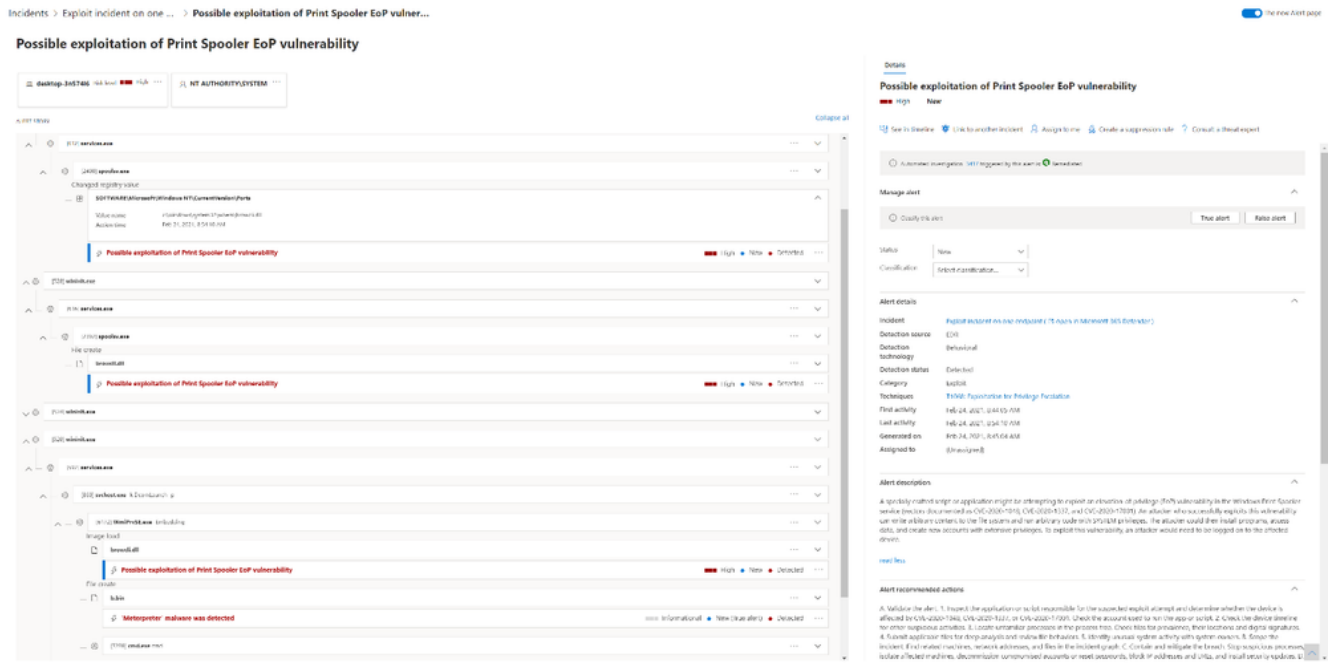


Figure 3. Detailed alert story showing steps of the attack and affected assets

Step 1: Add a new printer and a printer port

Let's say an attacker was able to determine that one of the devices in our fictional network has not yet been patched for CVE-2020-1048 and was able to log on to the device through an effective social engineering lure. The first phase of our exploitation scenario is for the attacker to add a new printer on this device called MS Publisher Color Printer. It is then associated to a new printer port which points to our targeted system file c:\windows\system32\wbem\browcli.dll.

```
PS C:\Windows\system32> Add-PrinterPort c:\windows\system32\wbem\browcli.dll
PS C:\Windows\system32> Add-Printer -Name "MS Publisher Color Printer" -DriverName "MS Publisher Color Printer" -PortNam
e c:\windows\system32\wbem\browcli.dll
PS C:\Windows\system32>
```

Figure 4. Printer and port creation

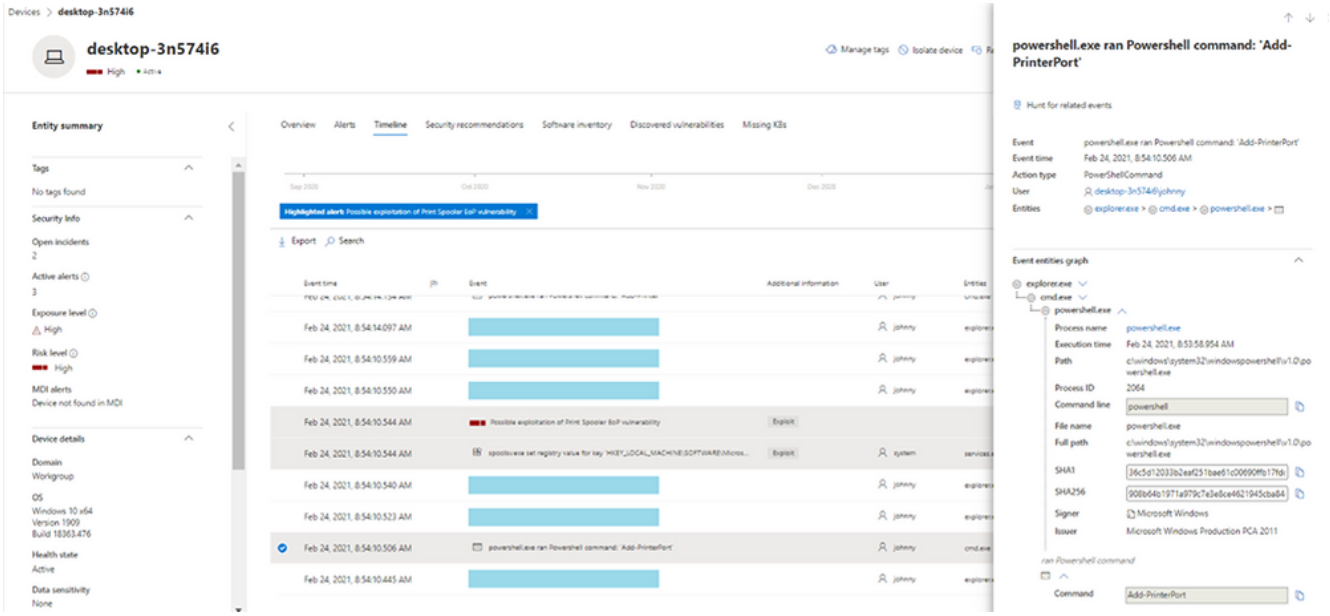


Figure 5. device timeline event showing the printer port was added

In the background, whenever a printer port is added, the spooler service adds a registry key containing the value of the path the user pointed to and where they would like to insert content. Since Defender for Endpoint monitors registry operations, it will detect this action as a suspicious registry activity right off the bat. The analyst will see the following alert:

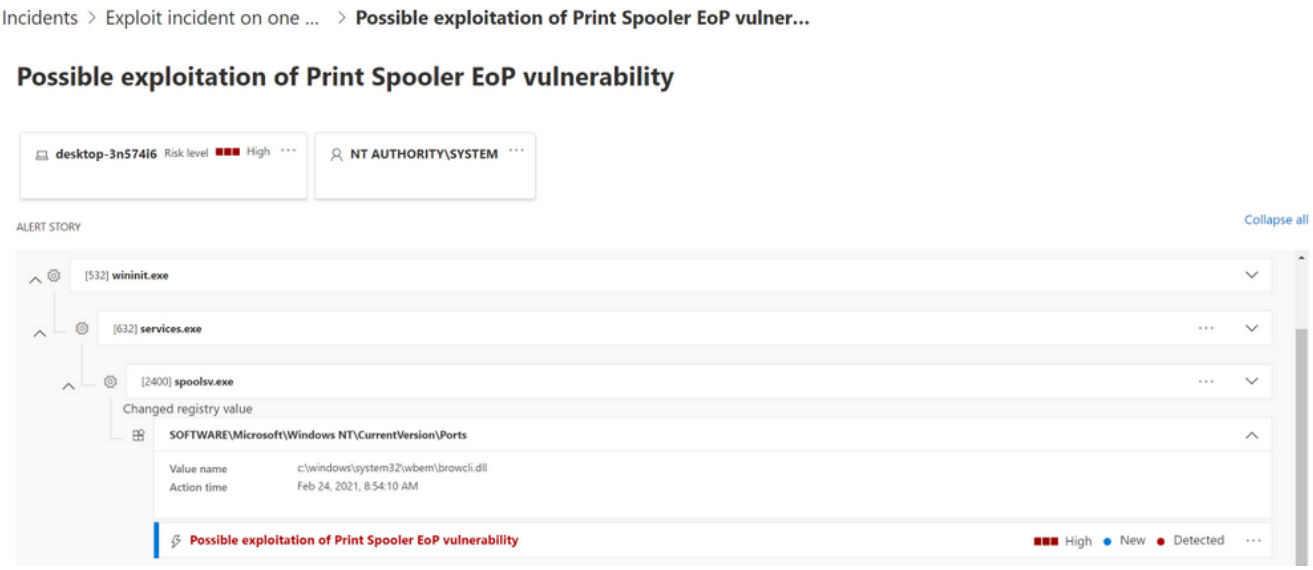


Figure 6. Alert flagging suspicious registry entry

Step 2: Print content to a restricted file

Typically, when a regular user creates a print job, the print job will be stored by the print spooler service (spoolsv.exe) to a dedicated folder, System32\SPOOL\Printers, as two files: the file, which contains the content to be printed, and the shadow job file (SHD), which contains the metadata of the print job, including the path of the printer port that was created. This same behavior is taken advantage of in this attack.

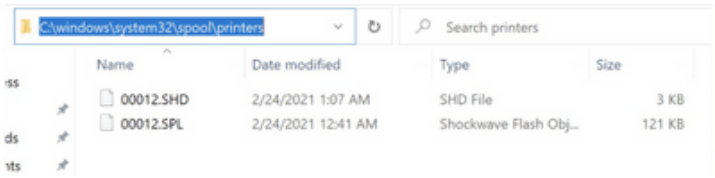


Figure 7. Print job creation

The core of this vulnerability is that through adding a printer port that points to the SYSTEM folder and by rebooting the spooler service, the attacker gets to run its malicious file when the spooler reloads, running as SYSTEM, and "prints" to the folder specified in the printer port.

SafeBreach Labs created proof-of-concept code on GitHub to generate one such crafted SHD file.

```
~/Downloads/SHDWriter > python SHDWriter.py ./inject
.dll "MS Publisher Color Printer" "MS Publisher Color Printer" "c:\\windows\\sys
tem32\\wbem\\browcli.dll" "NT AUTHORITY\SYSTEM" 10 DESKTOP DOCUMENT
[+] Opened payload file successfully
[+] Payload size is: 0x1e200
[+] Creating SHD file
[+] c:\windows\system32\wbem\browcli.dll
[*] File created successfuly: 00012.SHD
[*] Copy your payload file as: 00012.SPL, along with the generated SHD file
[+] Goodbye...
```

Figure 8. Sample SHD file

Now the attacker simply needs to wait for the print spooler to be initialized after a reboot. The print spooler then does its regular function of enumerating the SHD files folder so that it can process any remaining print jobs.

Process Name	PID	Operation	Path
spoolsv.exe	43500	QueryDirectory	C:\Windows\System32\spool\PRINTERS\FP*.SPL
spoolsv.exe	43500	QueryDirectory	C:\Windows\System32\spool\PRINTERS*.SHD

Figure 9. Print spooler enumerates unprocessed print jobs

In our exploitation scenario, the attacker was able to write arbitrary data to the path of the printer port which the attacker should not have had write access to. Just by copying the crafted SHD and SPL files and waiting for the system to reboot, the attacker achieved an elevation of privilege.

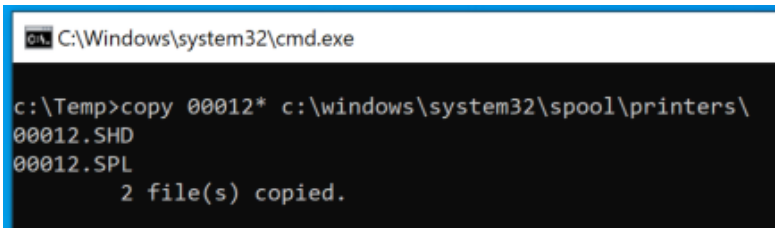


Figure 10. Attacker copies crafted print jobs files which triggers the vulnerability.

Fortunately, analysts will be made aware that this step was performed on the system because Defender for Endpoint will trigger and alert for the file creation of browcli.dll by the print spooler service.

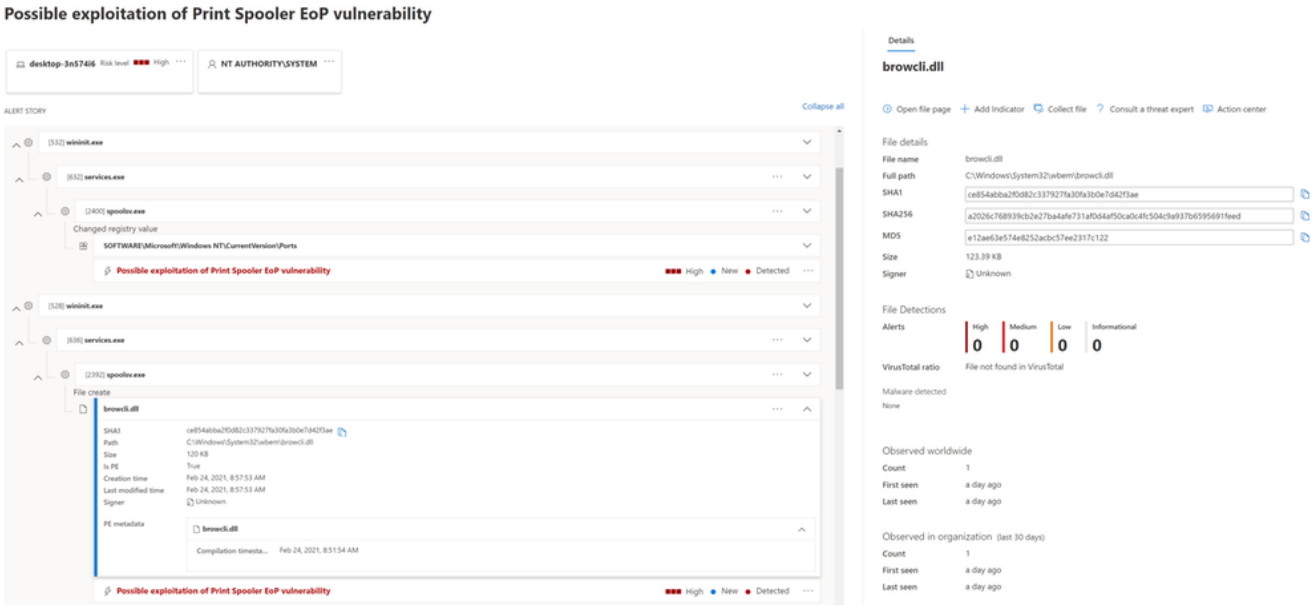


Figure 11. Alerts flagging suspicious file creation

Step 3: Perform DLL hijacking

In Windows environments, when an application or a service starts, it first loads several dependencies, also known as DLLs, to function properly. If these dependencies don't exist or are implemented in an insecure way, attackers could load and execute their malicious DLL instead.

In our attack scenario, the elevation of privilege allows code execution using DLL search order hijacking. The DLL actually contains a stager payload which reflectively (in-memory) loads a Meterpreter Reverse TCP shellcode over a TCP socket.

Once Windows is restarted, the WMI service (which is running as NT AUTHORITY\SYSTEM) will execute the browcli.dll library from the C:\Windows\System32\wbem folder, resulting in a reverse Meterpreter shell. This provides the attacker the ability to remotely steal information and propagate throughout more computers in the network, among others. The service executes the DLL every time the system reboots, so the attacker can use the vulnerability to elevate privileges.

In this case, thanks to the Defender for Endpoint registry, file, and load image sensors, we produced strong detection logic to identify suspicious behaviors indicating any attempt to exploit the vulnerability. At this point, the analyst assigned to this set of alerts will see the following alert story:

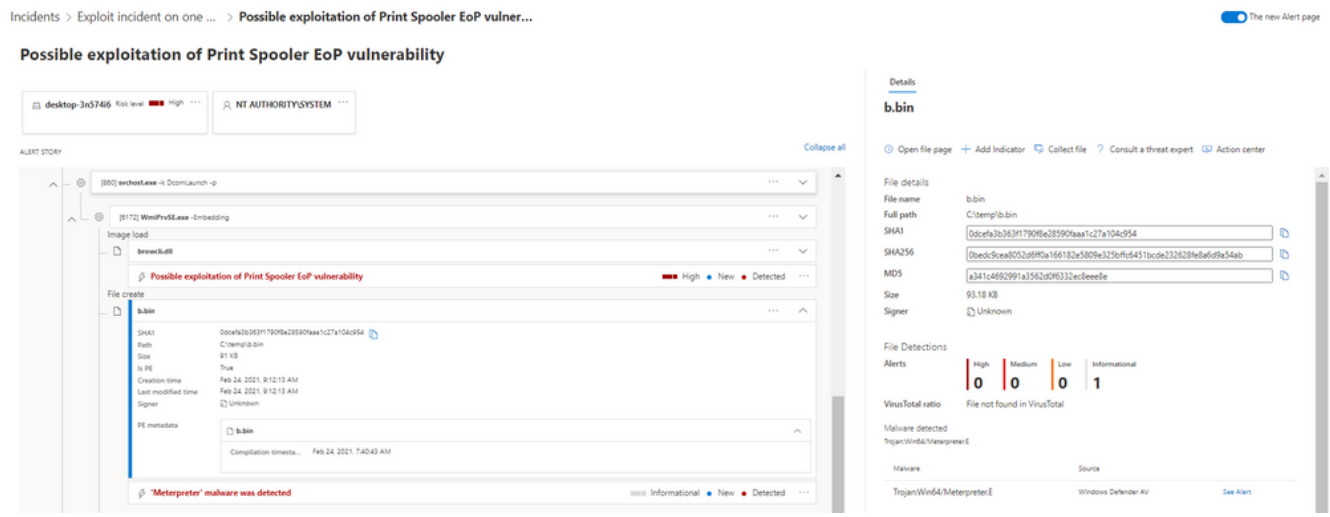


Figure 12. Alerts flagging suspicious 'Meterpreter' payload in memory

Please note that in this specific case we used an un-patched device, with the AV in passive-mode for the purpose of the simulation. If Defender AV was enabled, it would have blocked the malware before execution.

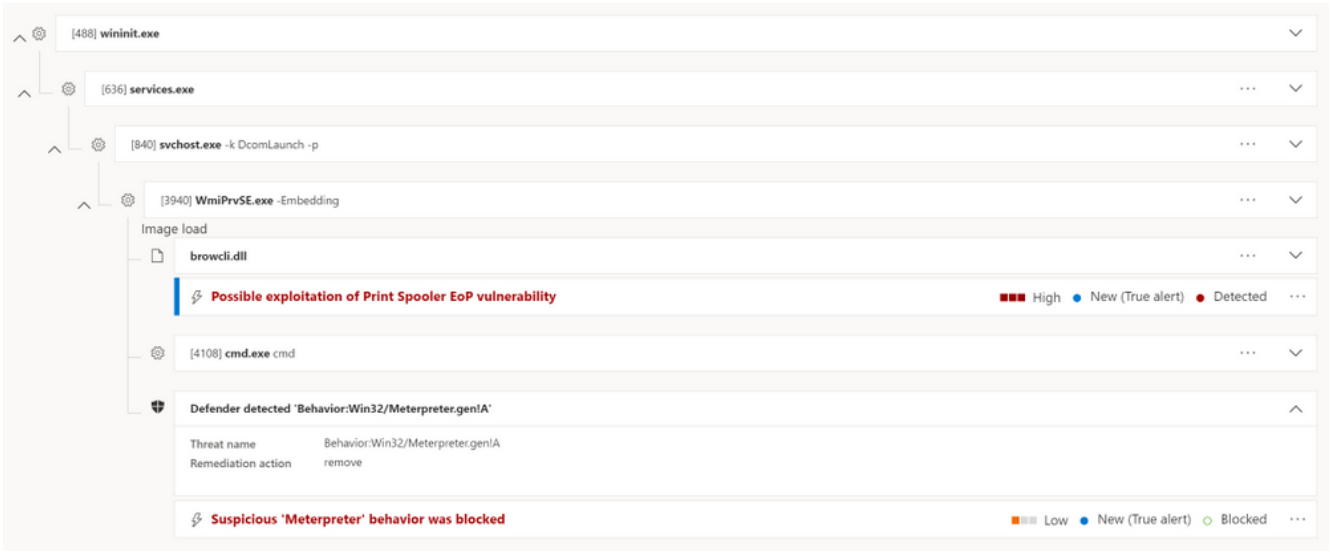


Figure 13. malicious 'Meterpreter' activity blocked by Defender AV

Seeing the attack story in one view

On top of the individual suspicious event detection, Defender for Endpoint provides an extensive attack storytelling capability. The incident page is the first stop of the security analyst, where they can learn about the scope of the attack, the related alerts, and the impacted entities across the organization, together with a full context of the investigation and remediation actions.

Diving in the new alert page, the full story of the suspicious registry activity by the printer port (detected by the EDR) followed by the Meterpreter file creation and the file loading events (detected by the AV) will be shown in the same detailed page, making the investigation more efficient and providing a better understanding of why the alerts were triggered—along with their impact.

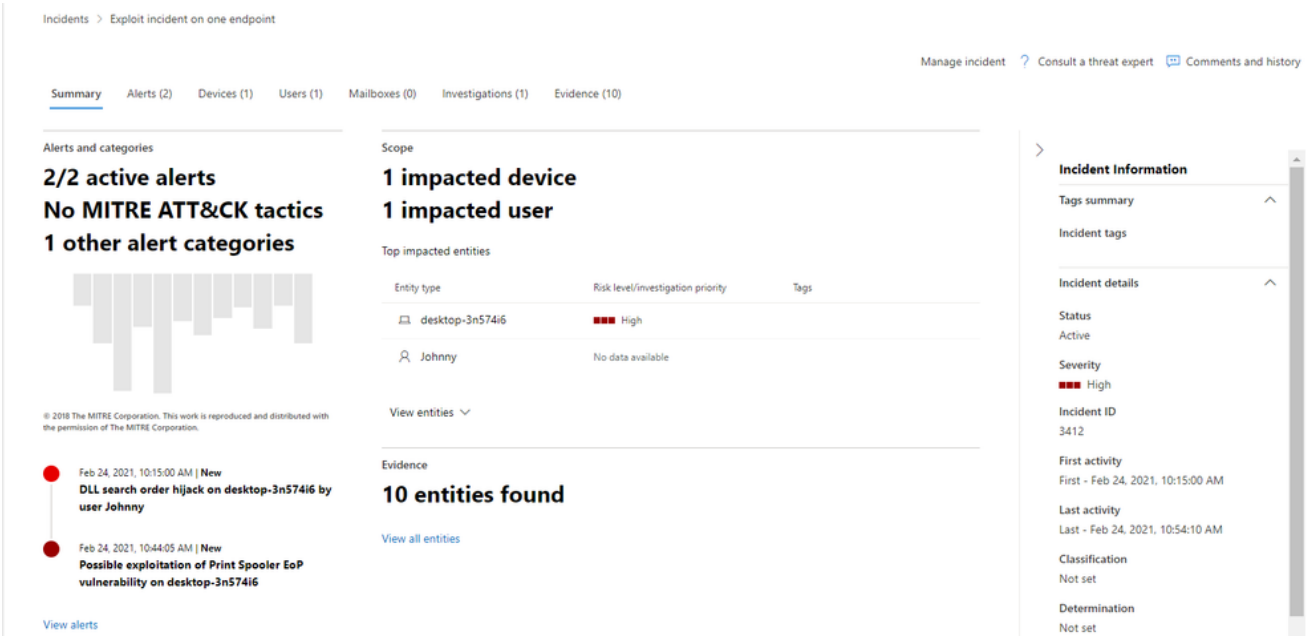


Figure 14. Analyst's first stop - the incident page

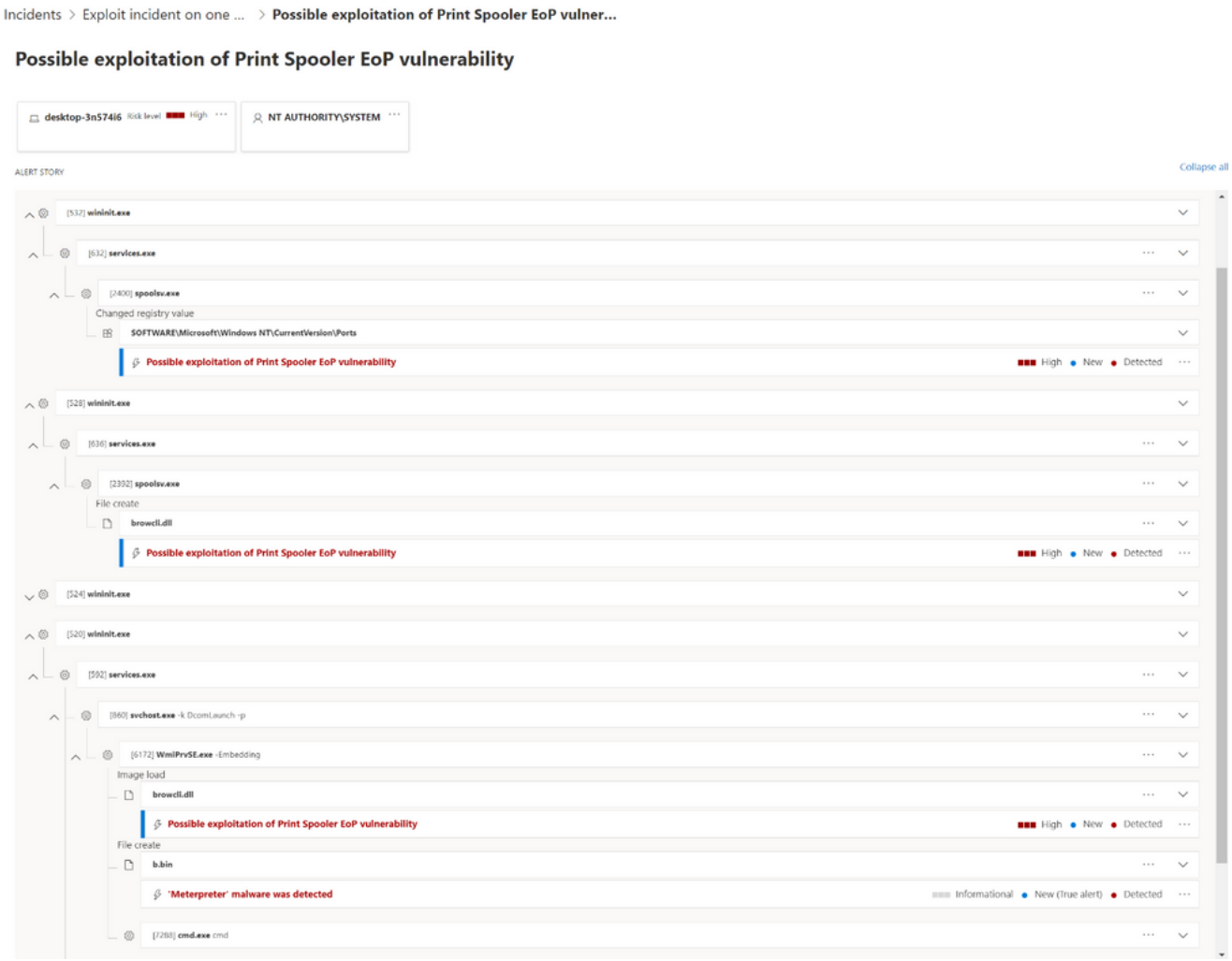


Figure 15. Full alert story of each step of the attack

This view of the correlation provides a full visualization of the attack goals and activities. The security operations team can clearly see that the alerts are related to the same sequence of events and thus can respond with the full attack context in mind.

The analyst can then drill down into the DLL tile, which is the malicious binary in this scenario, and see all the relevant details and actions, within the context of the investigation. Likewise, each tile in the alert story is expandable and shows more details in the side pane when clicked. Alert tiles are also actionable. By clicking on the "..." icon, available actions will be provided directly from the process tree.

Figure 16. Available actions provided directly from the alert story

By opening the automated investigation page, available both in the incident and the alert pages, the analyst can get a better understanding of the actions that were taken on the device, which assets where involved, and get all the related evidence.

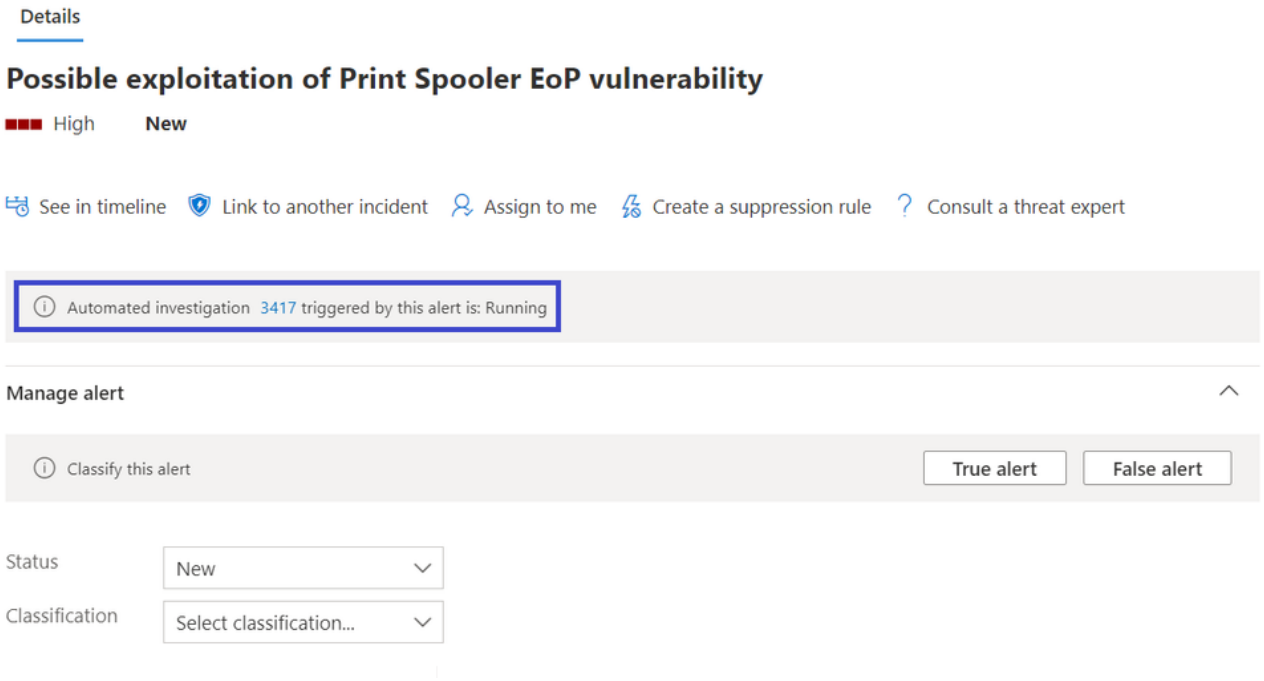


Figure 17. Alert details and actions

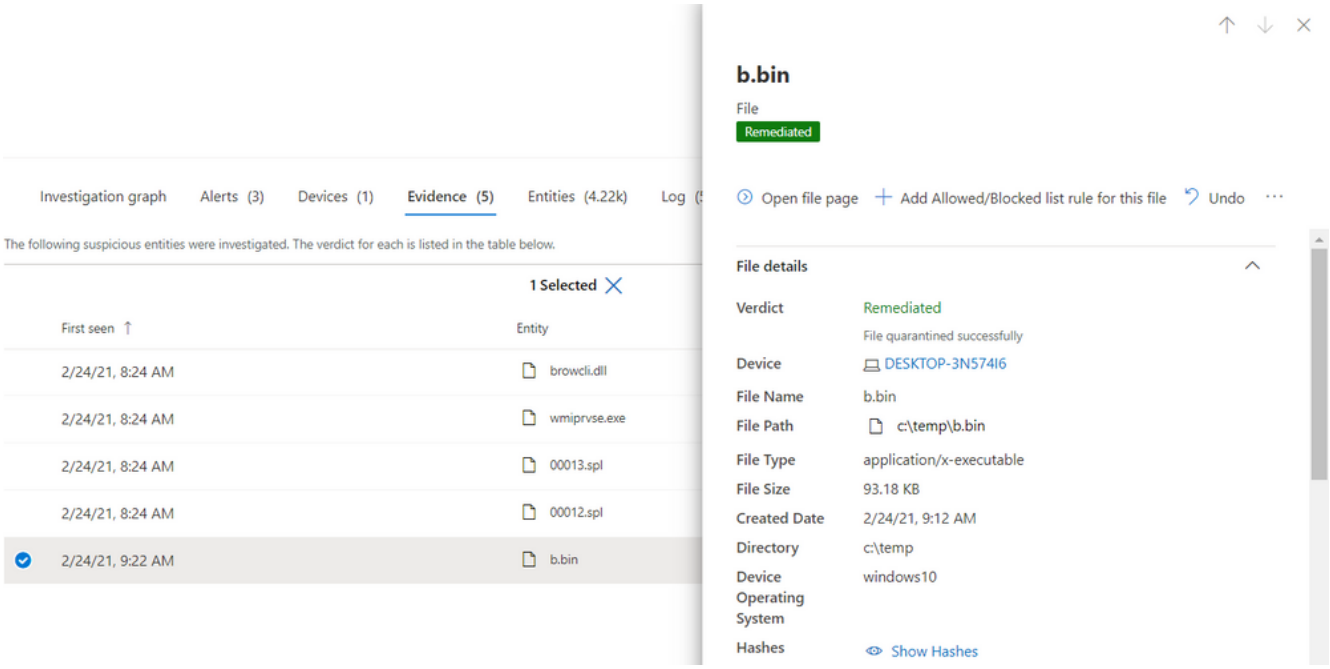


Figure 18. Automated investigation remediates and quarantines the malicious file

Searching for the vulnerability in Weaknesses page in Threat and Vulnerability Management will also help to identify all the other devices that might be vulnerable to spooler EoP:

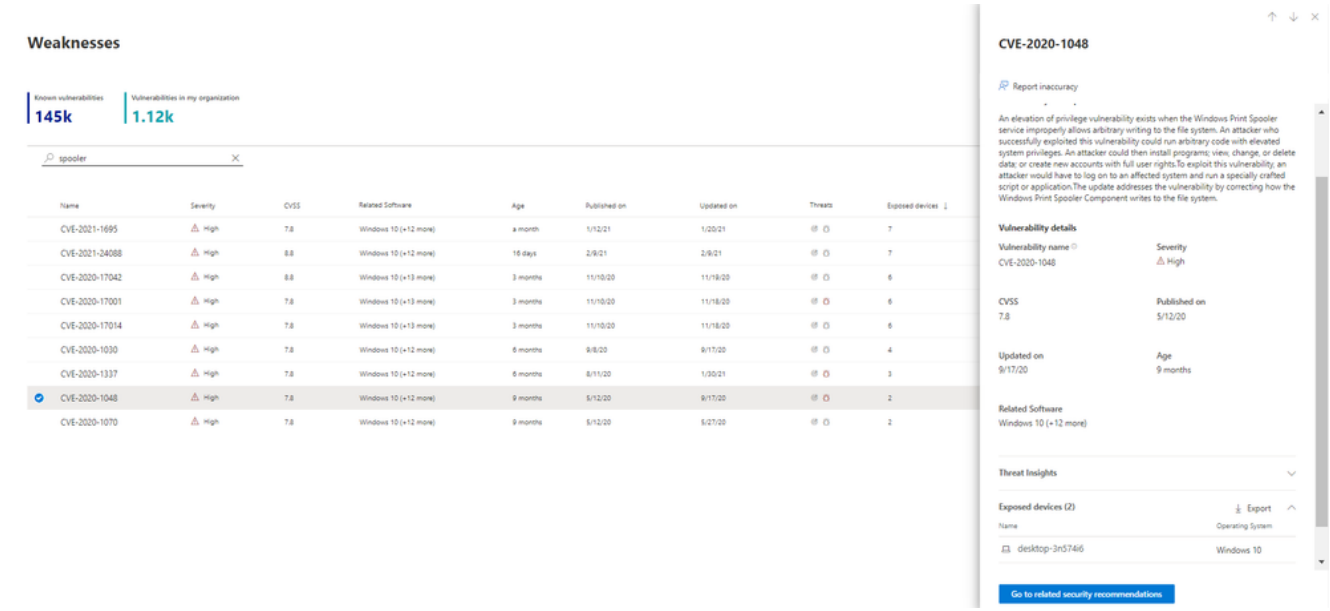


Figure 19. Exposed devices in weaknesses page

Furthermore, the details pane provides information about which MITRE ATT&CK technique was used in each step. These are incredibly useful in post-activity learning in incident response as it identifies which gaps exist in the current configuration of the network so the analyst can make recommendations to admins to improve security to avoid or lessen the impact of the next attack.

Figure 20. MITRE ATT&CK techniques and alerts flagged for each attacker step

As you have seen, using the SafeBreach attack simulations, Defender for Endpoint was able to detect the attack across the different kill-chain stages, provide a full investigation experience across detection and protection, including all data needed and by that telling the full alert story. The security operations team can explore all relevant details and take action on each related entity—without leaving the context of the alert investigation, designed to make the investigation experience efficient and easy.

To learn more about the new alert page, please read our documentation and blog post.

If you're not yet taking advantage of Microsoft Defender for Endpoint's industry leading security optics and detection capabilities, we encourage you to sign up for a free trial today.

Peleg Hadar SafeBreach Labs

Charles-Edouard Bettan & Yonit Glozshtein Microsoft Defender for Endpoint team

---

[i] Microsoft released fixes to address fix bypasses to CVE-2020-1048. These were documented as CVE-2020-1337 and CVE-2020-17001. While we are not discussing the details of those CVEs, the detection for CVE-2020-1048 also detects attempts to exploit CVE-2020-1337 and CVE-2020-17001.