# 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

#### Possible exploitation of Print Spooler EoP vulnerability

⊒ d	esktop-	3n574i6	5 Risk level 💵 High …	ℜ NT AUTHORITY\SYSTEM		
ALERT STO	ORY					Collapse al
^ ©	[532]	] wininit.o	exe			~
~	0	[632] <b>se</b> i	vices.exe		···	~
	^_ 4		400] <b>spoolsv.exe</b>			~
		Chan	ged registry value			_
		≌	SOFTWARE\Microsoft\Wind	lows NT\CurrentVersion\Ports		^
			Value name c:\w Action time Feb	vindows\system32\wbem\browcli.dll > 24, 2021, 8:54:10 AM		
			Possible exploitation	n of Print Spooler EoP vulnerability	High • New • Detected	

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 <u>updated Microsoft Defender for</u> <u>Endpoint alert page</u>, which has features to make the investigation experience better and more effective.

<u>SafeBreach</u>, one of our <u>evaluation lab partners</u> for breach and attack simulation solutions, discovered an <u>elevation of privilege</u> vulnerability in the Windows print spooler mechanism. This vulnerability, assigned <u>CVE-2020-1048[i]</u>, 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 <u>print spooler</u> 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.

Incidents > Exploit incident on one endpoint				
Summary Alerts (2) Devices (1) Users (1) N	Mailboxes (0) Investigations (1)	Evidence (10)	Manage incider	it ? Consult a threat expert 🖽 Comments and histo
Alerts and categories	Scope			>
2/2 active alerts	1 impacted devi	ce		Incident Information
No MITRE ATT&CK tactics	1 impacted user			Tags summary
1 other alert categories	Top impacted entities			Incident tags
	Entity type	Risk level/investigation priority	Tags	Incident details
	☐ desktop-3n574i6	High		Status Active
	Q Johnny	No data available		Severity
				High
© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation.	View entities 🗸			Incident ID 3412
Feb 24 2021 10:15:00 AM   New	Evidence			First activity
DLL search order hijack on desktop-3n574i6 by	10 entities found	ł		First - Feb 24, 2021, 10:15:00 AM
user Johnny				Last activity Last - Feb 24, 2021, 10:54:10 AM
Feb 24, 2021, 10:44:05 AM   New	view all entities			Classification
vulnerability on desktop-3n574i6				Not set
				Determination
View alerts				Not set

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

subjects of print Spoiler EoP vulnerability	tents > exploit inddent on one > Possible exploitation of Print Spooler EoP vulner	•	The new Alertip
	ossible exploitation of Print Spooler EoP vulnerability	Ditas	
	⊇ destep-3x67465 fill los tem film film film film film film film fil	Possible exploitation of Print Spooler EoP vulnerability = +iy> Ner	
i vienze	n 0500	Collapse al 😳 See is similare 🕷 Unit to another incident . 🔒 Ausyn to me 🚊 Cruate a suppression rule 🦩 Consult a thread expert	
<ul> <li>A distribution</li> &lt;</ul>	A O RU(service.com	··· •	
Implementation   Impl	A 0 2400 apodeses	O Administration Stiff togeneity that are to O tendeneity	
Version Version              Person        Person           Person           Person           Person           Person              Person           Person	Changed reprinty value	A Managa sket	^
	Volue name risarialise (sprime 3) sprime (simal) att. Automations Pre 21, 2211, 851 (829)	O deally the Alex Tex alex	trais sets
<ul> <li>International and the state of the state of</li></ul>	Possible exploitation of Mrd Spooler EoP valuerability	I I I I I I I I I I I I I I I I I I I	
A resultance in the large state of the large state is and results in the large state is and result is and	© [23] shears	Constitution factor canadication.	
A second seco	C RIN. BAYLOR. BID		^
Note Sector Sector   Note		Incident Expansion on the industry (it open in Microwy 165 Data April 2017) President April 2017	
Production of the space of t	N - 10 Unit sports	bataton televisial televisial	
A realise privation of the space Let a value shifty               Provide a regulation of the space Let a value shifty                Comparison	- D secondari	Detaction status Exclusion	
Produktion Produktio	Possible exploitation of Mint Spooler KoP veherability	Fight = Nos = Serving     Collegey     Laple     Trobelings     Trobelings     Trobelings     Trobelings	
Detailed and the standard of the standard o	[Dif white it as	Tinit activity 146-24, 2021, UAX 59-708	
p     p </td <td></td> <td>Last activity sets 24, 2021, 224 To AM</td> <td></td>		Last activity sets 24, 2021, 224 To AM	
<ul> <li>Notice in the set of the set of</li></ul>	(D3) which are	Generated on Reb 54, X92, R4556 AM     Assigned to (Directive R	
A 0 Bit reduces the strategy of the strateg	- © 1999 arrige are		
<ul> <li>In the trace is the first and is a set of the trace is th</li></ul>	A 0 Bill industrie Alternation g	Alert description     A social control over out available minist the elevering to control and addises (ToP) submatching the vehicles	A direct face der
Image load     Image load       Image load <td>~ = 0 statements</td> <td>service protons documented as OCO2005-040, OCO2005-040, OCO2005-040, OCO2005-040, And Andreas educ accountible equipois bio </td> <td>vulnerability ms, assess</td>	~ = 0 statements	service protons documented as OCO2005-040, OCO2005-040, OCO2005-040, OCO2005-040, And Andreas educ accountible equipois bio 	vulnerability ms, assess
	Image Load	data, and ceate new secounts with orderaive privileges. Its exploit this valuesability, an attacker would need to be logged on to the deriver.	e amochéd
Decision     Set     Constraint       0     Material     Material	$\hat{\mathcal{G}}$ . Prosible exploitation of Print Specier EoP vulnerability	red less	
Source of the state of the	The costs have	Alert tocommence actions	^
_ (interpretation of the second se	$\vec{\varphi}$ . Metospecter malware was detected	A Midde the Art. Unseet the spokation or both recorded replations to be recorded replationed and the rest of the spokation or both recorded replation and the the difference of the record rest of the spokation of the record rest of the record	device is evice timeline toi storaturos
	(S) [000] endurar mot	E. Sanit aptrace tist tr deparapit out index to the start. It to depara any out in the start of the star	do the Cost processes,

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.



### Figure 4. Printer and port creation

Devices > desktop-3n574i6						$\uparrow \downarrow$
desktop-3n574i	5		🔕 Manage t	ags 🚫 Isolate device 🧐 Ra	powershell.exe ra PrinterPort'	n Powershell command: 'Add-
Entity summary Tags	Cveniev Alerts Timeline	Security recommendations Software inventory: Discovered winesabilities 1	fissing KBs		<ul> <li>Hunt for related events</li> <li>Event powersh</li> <li>Event time Feb 24, 2</li> <li>Action type PowerSh</li> </ul>	ellese ran Powersheil command: 'Add-PrinterPort' 021, 854 10.506 AM BlCommand
No tags found Security Info Open incidents	Highlighted skets focube exploration of i	Verd and Annual Annua			User R deskto Entities © explor	po-3n5746iyohnny erexe > ⊚ omd.exe > ⊚ powershell.exe > □□
2 Active alerts ① 3	Bantina PEX CH, CUCI, GURLIGH ANN	p bet	Additional information	Der Entiles Openny Universit	Event entities graph © explorer.exe ~ L ond.exe ~ L powershell.exe	^
A High Risk level ⊙	Feb 24, 2021, 8:54:14:097 AM Feb 24, 2021, 8:54:10:559 AM			A johny esplorer A johny esplorer	Process name Execution time Path	powershell.exe Feb 24, 2021, 853:58.954 AM clwindowslaystem32/windowspowershellw1.0/po
MDI alerts Device not found in MDI	Feb 24, 2021, 8:54:10:550 AM			R johnny explorers	Process ID Command line	vershell.exe 2064 powershell
Device details	Feb 24, 2021, 854/10.544 AM	<ul> <li>Positive explosizion of new spores to inversions</li> <li>sportowne set reporty value for kay 'HET', LOCAL, MACHINESOFTORREMICON.</li> </ul>	bpot	R system services.c	File name Full peth	powershell.exe clwindowslaystem32/windowspowershell/u1.0.po wershell.exe [2644413033303/ave/043304614000096613264]
05 Windows 10 x64	Feb 24, 2021, 8:54:10:540 AM			R jammy explorers R jammy explorers	SHA256 Signer	900b64b1971a979c7e3e8ce4621945cba84
Version 1909 Build 18363.476 Health state	Feb 24, 2021, 8:54:10:506 AM	poventellaes on Poventel command: Xdd-Poresford		R johnny and eve	Issuer	Microsoft Windows Production PCA 2011
Active Data sensitivity None	Feb 24, 2021, 8:54:10:445 AM			R johnny explorers	Command	Add-PrinterPort

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:

Incidents > Exploit incident on one ... > Possible exploitation of Print Spooler EoP vulner...

#### Possible exploitation of Print Spooler EoP vulnerability

😐 desktop	p-3n574i6	Risk level 💶 High …	♀ NT AUTHORITY\SYSTEM …		
ALERT STORY					Collapse a
∧ <sup>©</sup> [53	32] wininit.e	xe			~
~ - @	[632] ser	vices.exe			~
~	(24	00] spoolsv.exe			~
	Chang B	software\Microsoft\Wind	lows NT\CurrentVersion\Ports		^
		Value name C\v Action time Feb	vindows\system32\wbem\browcli.dll b 24, 2021, 8:54:10 AM		
		Solution	of Print Spooler EoP vulnerability	High • New • Detected	

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.



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 43500	QueryDirectory	C:\Windows\System32\spool\PRINTERS\FP*.SPL 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.

Possible exploitation of Print Spooler EoP vulnerability

				Details		
🖾 desktop-3n57486 Risk level 🎫 High … 🔗	NT AUTHORITY\SYSTEM			browcli.dll		
ALERE STORY			Collapse all	Open file page	+ Add Indicator 🦻 Collect file 🦩 Consult a threat expert 🔯 Action center	
(532) windoit.exe           (532) services.exe			× ×	File details File name Full path	browcli.dll C:\Windows/System32(wbem/browcli.dll	
Changed registry value B SOFTWARE(MicrosoftWindows N C Possible exceptation of Pr	November Sector	Mich New Distected	× ×	SHA1 SHA256 MDS Size	0455480620082c319927103008200F35473ae 82026c7680390c32e27ba4a6731at064at50ac04f504c14e337b6595691feed e12ae63e574e8253ac0c57ee2317c122 123.39 KB b104exem	
(321) winisit.exe           (321) service.exe			* *	File Detections Alerts	tigh Medium Low Informational 0 0 0 0	
File create			~	VirusTotal ratio Malware detected None	File not found in VirusTotal	
SHA1         cel54abb           Path         CUWide           Size         120 KB           In P         Tour           Crastion time         Feb 24.20           Last modified time         Feb 24.20           Signer         D Ustance	Dolaniza (1997/1906/Biologi Addita) Gfynen 22 uder Hannell (dl 11, 8575) AM 11, 8575) AM			Observed worldwi Count First seen Last seen	de 1 a day ago a day ago	
PE metadata D brow Compil	ch.eff		^	Observed in organ Count First seen	ization (set 30 days) 3 a day ago	
Possible exploitation of Pr	int Spooler EoP vulnerability	High   New   Detected		same secol		

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 <u>elevation of privilege</u> allows <u>code execution</u> using <u>DLL search order</u> <u>hijacking</u>. 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:

Incidents > Exploit incident on one ... > Possible exploitation of Print Spooler EoP vulner...



#### Possible exploitation of Print Spooler EoP vulnerability

🗆 desktop-3n574i6	Risk	evel 🞫 High ····	O NT AUTHORITOSYSTEM ····					Details			
ALERT STORY						Collaps	se all	<ul> <li>Open file page</li> </ul>	+ Add Indicator	Gollect file ? Consult a threat expert 🕞 Action or	mber
	2) such	nostaxe -k DcomLaunch -	¢			×	^	File details File name Full path	b.bin C/temo/b.bin		
	nagel	load browclidtt	oony			~		SHA1 SHA256	Odcefa3b363f1790f Obedc9cea8052d6ff	18e28590faaa1c27a104c954 H0a166182e5809e325bffc6451bcde232628fe8a6d9a54ab	
Fi	ile cre	Possible exploit tote b.bin	ation of Print Spooler EoP vulnerability	High • New • Detec	yh e New e Detected         MD5         [a341:d6903991a3562a0f6032ec0eeele           Size         93.18.08           Size         03.18.08			i2d0f6332ec8eee8e	0		
		SHA1 Path Size Is PE Creation time Last modified time Signer	OccursIo030171700fe20390feastc219106c954 D Creenplace 91:03 The Res 54, 2021; 91:21:3 AM Res 54, 2021; 91:21:3 AM Res 54, 2021; 91:21:3 AM Diverselan Diverselan				l	File Detections Alerts VirusTotal ratio	High Medium 0 0	Low Informational 0 1 usfotal	
		PE metadata Compilation timesta Feb 24 3021,74043 AM				^	L	Malware detected Trojan/Win64/Meterprete Malware	el.	Source	
		§ 'Meterpreter' m	alware was detected	Informational • New • Detec	cted			Trojan:Win64/Mete	rpreter.£	Windows Defender AV See Aler	

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.

lerts and catenories	Scope			
2/2 active alerts	1 impacted devi	ce.		Incident Information
No MITRE ATT&CK tactics	1 impacted user			Tags summary
other alert categories	Top impacted entities			
	Entity type	Risk level/investigation priority	Tags	Incident details
	☐ desktop-3n574i6	High		Status
	A Johnny	No data available		Severity
				High
2018 The MITRE Corporation. This work is reproduced and distributed with e permission of The MITRE Corporation.	View entities $\checkmark$			Incident ID 3412
	Evidence			First activity
DLL search order hijack on desktop-3n574i6 by	10 entities found	d		First - Feb 24, 2021, 10:15:00 AM
user Johnny				Last activity Last - Feb 24, 2021, 10:54:10 AM
Feb 24, 2021, 10:44:05 AM   New	View all entities			Classification
Possible exploitation of Print Spooler EoP vulnerability on desktop-3n574i6				Not set

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

Incidents > Exploit incident on one ... > Possible exploitation of Print Spooler EoP vulner...

#### Possible exploitation of Print Spooler EoP vulnerability

desktop-3n!	57416 Rid	klevel 🎫 High \cdots			
ALERT STORY					Collapse a
∧ ◎ [532] wir	init.exe				× 1
∧ © [6]	2] services	Lexe			~
~_ ©	[2400] <b>s</b>	poolsv.exe			~
c	thanged r	registry value DFTWARE\Microsoft\Win	dows NT\CurrentVersion\Ports		~
	ş	Possible exploitatio	n of Print Spooler EoP vulnerability	High • New • Detected	
∧ () [528] wir	ninit.exe				~
∧ © [63	6] services	.exe			~
~ 0	[2392] <b>s</b>	poolsv.exe			~
F	ile create	rowclLdll			~
	ş	Possible exploitatio	n of Print Spooler EoP vulnerability	High • New • Detected	
√ ◎ [524] wir	alnit.exe				~
∧ ◎ [520] wir	init.exe				~
A @ [22	2] services	Lexe			~
∧ — ©	[860] <b>s</b> w	chost.exe -k DcomLaunch	т-р		~
~	@ [6	172] WmlPrvSE.exe -Emb	edding		~
	Imag — 🗋	e load browcli.dll			~
		& Possible exploi	itation of Print Spooler EoP vulnerabili	ty High • New • Detected	•••
	- D	b.bin			~
			nalware was detected	Informational   New (true alert)  Detected	
	0	[7283] cmd.exe cmd			~

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.

∧ ◎ [528] wininit.exe	Open file page				
	+ Add Indicator				
[636] services.exe					
∧ _ ⊚ [2392] spoolsv.exe	? Consult a threat expert				
File create					
browcii.dll	~ ~				
Possible exploitation of Print Spooler EoP vulnerability					

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.

Details									
Possible exploitation of Print Spooler EoP vulnerability									
High N	ew								
🗟 See in timeline	e 💿 Link to another incident	8 Assign to me	<sup>7</sup> / <sub>∞</sub> Create a suppression rule	? Consult a threat e	expert				
(i) Automated i	nvestigation 3417 triggered by this a	lert is: Running							
Manage alert					^				
(i) Classify this a	alert			True alert	False alert				
		7							
Status	New 🗸								
Classification	Select classification $\checkmark$								

Figure 17. Alert details and actions

					$\uparrow  \downarrow$
			b.bin		
			File Remediated		
Investigation graph A	lerts (3) Devices (1)	Evidence (5) Entities (4.22k)	Log (! 💿 Open file p	age $+$ Add Allowed/Blocked list rule for this file	") Undo
e following suspicious entities wer	e investigated. The verdict for ea	ch is listed in the table below.	File details		^
		1 Selected 🗙	Verdict	Remediated	
First seen ↑		Entity	veraice	File quarantined successfully	
2/24/21, 8:24 AM		D browcli.dll	Device	DESKTOP-3N574I6	
		D	File Name	b.bin	
2/24/21, 8:24 AM		wmiprvse.exe	File Path	🗅 c:\temp\b.bin	
2/24/21, 8:24 AM		D 00013.spl	File Type	application/x-executable	
		D	File Size	93.18 KB	
2/24/21, 8:24 AM		00012.spl	Created Date	2/24/21, 9:12 AM	
2/24/21, 9:22 AM		🗋 b.bin	Directory	c:\temp	
			Device Operating System	windows10	
			Hashes	Show Hashes	

Figure 18. Automated investigation remediates and quarantines the malicious file

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

Weaknesses									CVE 2020 1049	Υ V	×
Koons witheredities in my organization           145k         1.12k								CVE-2020-1048		•	
_⊖ spooler Name	X Servity CvSS Rested Software Age Rublished on Updated on 77metra Bupteed devices (							system privilege. An attacker could then initial programs view, change, or delate date or oreal new accounts this ful user rights regulation this valender attacker mould have to log on to an affected system and run a specially confined script or application/The update address the valentality by correcting how the Windows Print Speciel Component writes to the file system.			
CVE-2021-1695	A High	7.8	Windows 10 (+12 more)	a month	1/12/21	1/20/21	@ 0	7	Vulnerability details		
CVE-2021-24088	A High	8.8	Windows 10 (+12 more)	16 days	2/9/21	2/9/21	0 0	,	Vulnerability name  CVE-2020-1048	Severity High	
CVE-2020-17042	A High	8.8	Windows 10 (+13 more)	3 months	11/10/20	11/18/20	0 0	6			
CVE-2020-17001	A High	7.8	Windows 10 (+13 more)	3 months	11/10/20	11/18/20	0 0	6	CVSS 7.8	Published on	
CVE-2020-17014	A High	7.8	Windows 10 (+13 more)	3 months	11/10/20	11/18/20	0 0	6		5/12/20	
CVE-2020-1030	A High	7.8	Windows 10 (+12 more)	6 months	9/8/20	9/17/20	00	4	Updated on	Age	
CVE-2020-1337	A High	7.0	Windows 10 (+12 more)	6 months	8/11/20	1/30/21	@ <b>0</b>	3	9/17/20	9 months	
CVE-2020-1048	A High	7.8	Windows 10 (+12 more)	9 months	\$/12/20	9/17/20	0 0	2	Related Software		
CVE-2020-1070	A High	7.8	Windows 10 (+12 more)	9 months	\$/12/20	\$/27/20	0 0	2	Windows 10 (+12 more)		
									Threat Insights	~	1
									Exposed devices (2)	± Export	
									Name	Operating System	
									.⊟. desktop-3n574i6	Windows 10	
											•
									Go to related security recomme	endations	

### 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.