



# High Vulnerability Report

---

## Overview:

Shade+ is a thick client application developed using Apeon 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

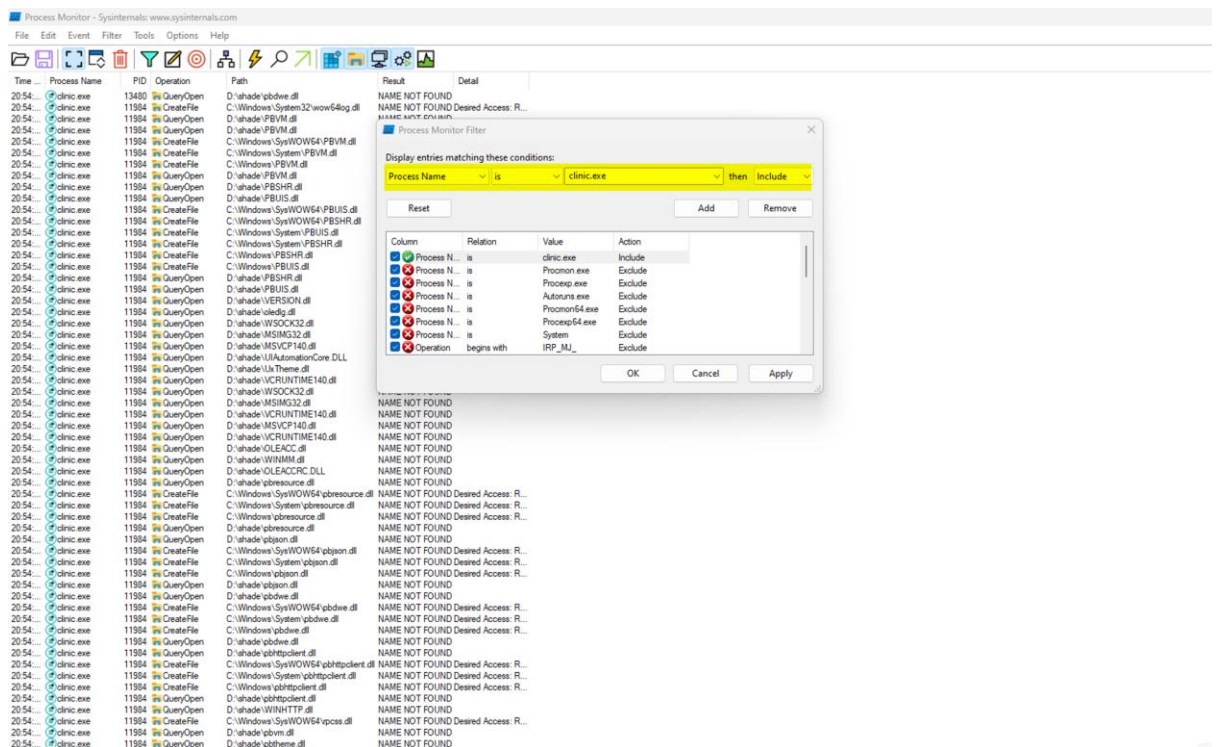
1. Launch "Process monitor" tool and filter the result to display all the activities related to "Clinic.exe" with path ending with ".dll" and result contains "NAME NOT FOUND"
2. Launch the shade application and observe the application searching for "pbresource.dll" in the current directory.
3. Generate 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:



The screenshot shows the Process Monitor tool interface. The main window displays a list of events filtered for 'clinic.exe'. The filter dialog is open, showing the filter criteria: 'Process Name is clinic.exe'. The main window displays a list of events with columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The filter dialog also shows a table of columns and their actions.

Column	Relation	Value	Action
Process N...	is	clinic.exe	Include
Process N...	is	Processp.exe	Exclude
Process N...	is	Autounst.exe	Exclude
Process N...	is	Process64.exe	Exclude
Process N...	is	System	Exclude
Operation	begins with	IRP_MJ_	Exclude

## 2. Filtering path end with .dll file:

The screenshot shows the Process Monitor application window. The main pane displays a list of system events, all of which are filtered to show only those where the path ends with ".dll". The filter dialog box is open, showing the condition: "Path ends with \\.dll then Include". The "Columns" tab is selected, showing a table of columns and their actions:

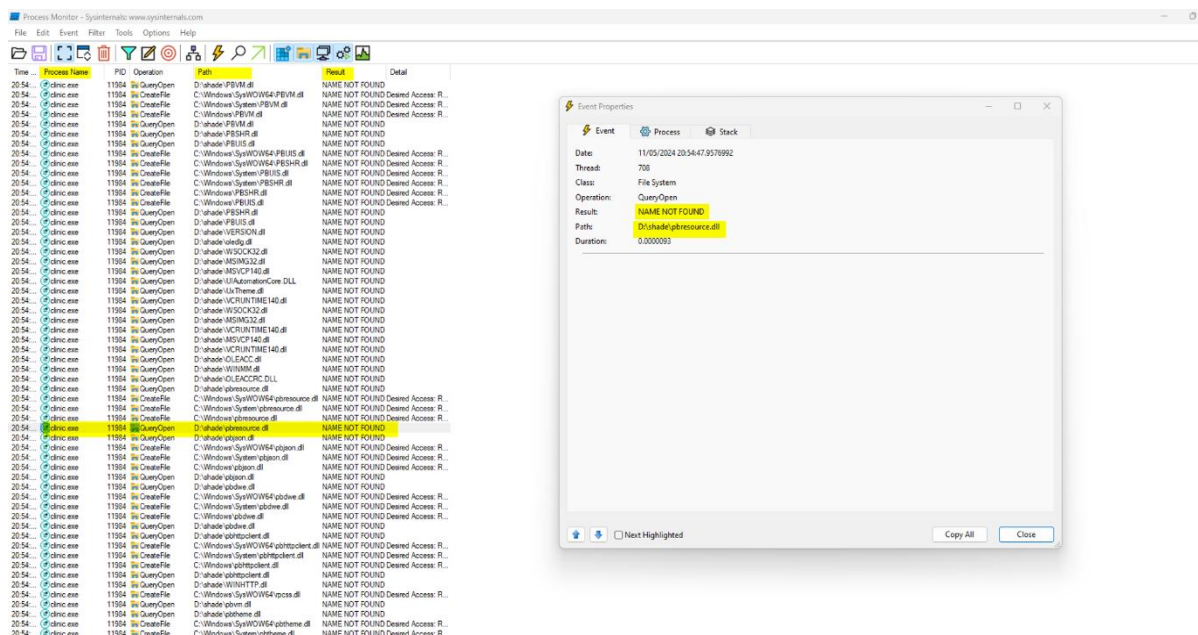
Column	Relation	Value	Action
Process N...	is	clnic.exe	Include
Result	contains	NAME NOT FO...	Include
Process N...	is	Procmon.exe	Exclude
Process N...	is	Autounst.exe	Exclude
Process N...	is	Procmon64.exe	Exclude
Process N...	is	System	Exclude

## 3. Filtering result contains "NAME NOT FOUND":

The screenshot shows the Process Monitor application window with the filter dialog box open. The filter condition is now: "Result contains 'NAME NOT FOUND' then Include". The "Columns" tab is selected, showing the same table as in the previous screenshot, but with the "Result" column's action set to "Include":

Column	Relation	Value	Action
Process N...	is	clnic.exe	Include
Result	contains	NAME NOT FO...	Include
Process N...	is	Procmon.exe	Exclude
Process N...	is	Autounst.exe	Exclude
Process N...	is	Procmon64.exe	Exclude
Process N...	is	System	Exclude

#### 4. Pbresource not found in the result:



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

```
D:\metasploit-framework\bin>msfvenom -f dll -p windows/exec CMD="C:\Windows\System32\calc.exe" -o pbresource.dll
D:\metasploit-framework\embedded\lib\ruby\gems\3.0.0\gems\ruby-core-0.1.31\lib\rex\compat.rb:381: warning: Win32API is deprecated after Ruby 1.9.1
; use fiddle directly instead
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 213 bytes
Final size of dll file: 9216 bytes
Saved as: pbresource.dll
```

### 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.