REDBACK OPERTAIONS

VULNERABILITY FOUNDED-Failure to Handle COM Initialization Failure

Name	Team	Role	Is this a re-tested Finding?
Pranav Sharma	Cybersecurity team	Secure code team	No

Was this Finding Successful?
Yes

Risk Rating

Impact: Moderate
Likelihood:Unlikely

Impact values				
Very Minor	**Minor**	**Significant**	**Major**	**Severe**
Risk that holds little to no impact. Will not cause damage and regular activity can continue.	Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity.	Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally.	Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally.	Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run.

Likelihood				
Rare	**Unlikely**	**Moderate**	**High**	**Certain**
Event may occur and/or if it did, it happens in specific circumstances.	Event could occur occasionally and/or could happen (at some point)	Event may occur and/or happens.	Event occurs at times and/or probably happens a lot.	Event is occurring now and/or happens frequently.

Business Impact

If COM initialization fails, it could lead to unexpected behavior or crashes in the application. This could impact user experience and potentially lead to loss of trust in the application.

Location of vulnerability
inside the "wWinMain" function

Evidence

```
    FlutterWindow window(project);
    Win32Window::Point origin(10, 10);
    Win32Window::Size size(1280, 720);
    if (!window.Create(L"vcapp", origin, size)) {
      return EXIT_FAILURE;
    }
    window.SetQuitOnClose(true);

    ::MSG msg;
    while (::GetMessage(&msg, nullptr, 0, 0)) {
      ::TranslateMessage(&msg);
      ::DispatchMessage(&msg);
    }

    ::CoUninitialize();
    return EXIT_SUCCESS;
}
```

Remediation Advice

Implement proper error handling for the CoInitializeEx call. If initialization fails, release any resources allocated before returning from the wWinMain function.

Add error handling for console attachment failure, providing appropriate feedback or fallback mechanisms for debugging purposes.

Contact Details

Pranav Sharma

S222208296