REDBACK OPERTAIONS

VULNERABILITY FOUNDED -Unhandled window messages

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: Minor

Likelihood: Rare

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.

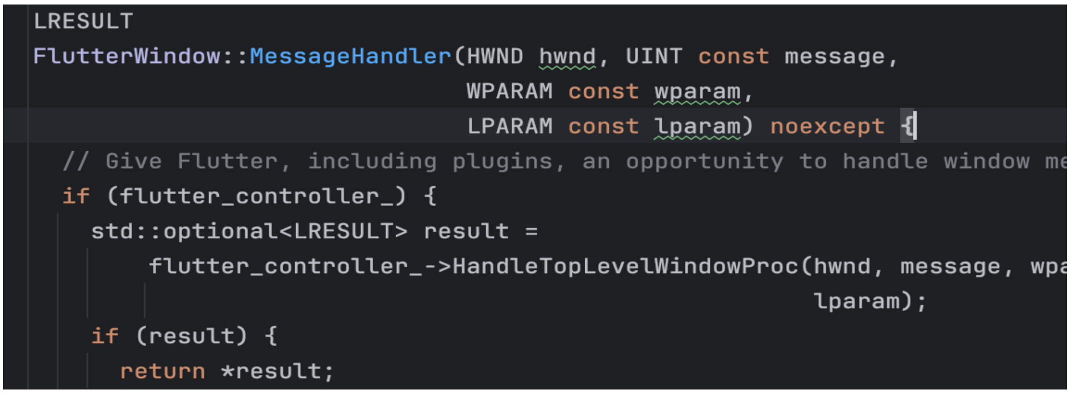
Business Impact

If certain window messages are not handled correctly by Flutter or its plugins, it could lead to unexpected behaviour or crashes in the application. However, the impact is likely to be minor since it's specific to window message handling.

Location of vulnerability

Inside the MessageHandler function.

Evidence



```
LRESULT
FlutterWindow::MessageHandler(HWND hwnd, UINT const message,
                              WPARAM const wparam,
                              LPARAM const lparam) noexcept {
  // Give Flutter, including plugins, an opportunity to handle window me
  if (flutter_controller_) {
    std::optional<LRESULT> result =
        flutter_controller_->HandleTopLevelWindowProc(hwnd, message, wpa
                                                      lparam);
    if (result) {
      return *result;
```

Remediation Advice

Ensure that all relevant window messages are properly handled by Flutter and its plugins to prevent unexpected behaviour or crashes.

Implement robust error handling and logging mechanisms to detect and diagnose any issues related to window message handling.

Contact Details

Pranav Sharma
S222208296