# Final Summary

## Summary

This C++ code performs DLL injection into a specified process on Windows. It gets a handle to the target process, allocates memory within it, writes the path of a DLL into the allocated memory, and creates a new thread that calls LoadLibraryA with the DLL path. This causes the target process to load the specified DLL.

## Security Concerns

Yes

## Security Rating

High

## Rating Justification

The code allows arbitrary DLL injection into a process with a user-specified PID, which can be a serious security concern. This technique is often used for malicious purposes such as process manipulation or data extraction. If the DLL specified contains malicious code, it can compromise the integrity, confidentiality, and availability of the target process and potentially the entire system. Therefore, the security rating is high.

# C:\Users\Jason.Adkin\Projects\Malicious\_Code\_Examples\Cpp\_Example.c

## Summary

This C++ code performs DLL injection into a specified process on Windows. It gets a handle to the target process, allocates memory within it, writes the path of a DLL into the allocated memory, and creates a new thread that calls LoadLibraryA with the DLL path. This causes the target process to load the specified DLL.

## Security Concerns

Yes

## Security Rating

High

## Rating Justification

The code allows arbitrary DLL injection into a process with a user-specified PID, which can be a serious security concern. This technique is often used for malicious purposes such as process manipulation or data extraction. If the DLL specified contains malicious code, it can compromise the integrity, confidentiality, and availability of the target process and potentially the entire system. Therefore, the security rating is high.