**枚举所有进程**

* 项目
* 2023/06/12
* 7 个参与者

反馈

以下示例代码使用 [**EnumProcesses**](https://learn.microsoft.com/zh-cn/windows/win32/api/Psapi/nf-psapi-enumprocesses) 函数检索系统中每个进程对象的进程标识符。 然后调用 [EnumProcessModules](https://learn.microsoft.com/zh-cn/windows/win32/api/psapi/nf-psapi-enumprocessmodules) 以获取每个进程名称并打印它。

**备注**

对于 64 位进程，请使用 [**EnumProcessModulesEx**](https://learn.microsoft.com/zh-cn/windows/win32/api/psapi/nf-psapi-enumprocessmodulesex) 函数。

C++

#include <windows.h>

#include <stdio.h>

#include <tchar.h>

#include <psapi.h>

// To ensure correct resolution of symbols, add Psapi.lib to TARGETLIBS

// and compile with -DPSAPI\_VERSION=1

void PrintProcessNameAndID( DWORD processID )

{

TCHAR szProcessName[MAX\_PATH] = TEXT("<unknown>");

// Get a handle to the process.

HANDLE hProcess = OpenProcess( PROCESS\_QUERY\_INFORMATION |

PROCESS\_VM\_READ,

FALSE, processID );

// Get the process name.

if (NULL != hProcess )

{

HMODULE hMod;

DWORD cbNeeded;

if ( EnumProcessModules( hProcess, &hMod, sizeof(hMod),

&cbNeeded) )

{

GetModuleBaseName( hProcess, hMod, szProcessName,

sizeof(szProcessName)/sizeof(TCHAR) );

}

}

// Print the process name and identifier.

\_tprintf( TEXT("%s (PID: %u)\n"), szProcessName, processID );

// Release the handle to the process.

CloseHandle( hProcess );

}

int main( void )

{

// Get the list of process identifiers.

DWORD aProcesses[1024], cbNeeded, cProcesses;

unsigned int i;

if ( !EnumProcesses( aProcesses, sizeof(aProcesses), &cbNeeded ) )

{

return 1;

}

// Calculate how many process identifiers were returned.

cProcesses = cbNeeded / sizeof(DWORD);

// Print the name and process identifier for each process.

for ( i = 0; i < cProcesses; i++ )

{

if( aProcesses[i] != 0 )

{

PrintProcessNameAndID( aProcesses[i] );

}

}

return 0;

}

main 函数使用 [**EnumProcesses**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Psapi/nf-psapi-enumprocesses) 函数获取进程列表。 对于每个进程，main调用 **PrintProcessNameAndID** 函数，向其传递进程标识符。 **PrintProcessNameAndID** 依次调用 [**OpenProcess**](https://learn.microsoft.com/zh-cn/windows/desktop/api/processthreadsapi/nf-processthreadsapi-openprocess) 函数以获取进程句柄。 如果 **OpenProcess** 失败，输出会将进程名称显示为 <未知>。 例如，对于 Idle 和 CSRSS 进程， **OpenProcess** 会失败，因为它们的访问限制阻止用户级代码打开它们。 接下来， **PrintProcessNameAndID** 调用 [**EnumProcessModules**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Psapi/nf-psapi-enumprocessmodules) 函数以获取模块句柄。 最后， **PrintProcessNameAndID** 调用 [**GetModuleBaseName**](https://learn.microsoft.com/zh-cn/windows/desktop/api/Psapi/nf-psapi-getmodulebasenamea) 函数以获取可执行文件的名称，并显示名称以及进程标识符。