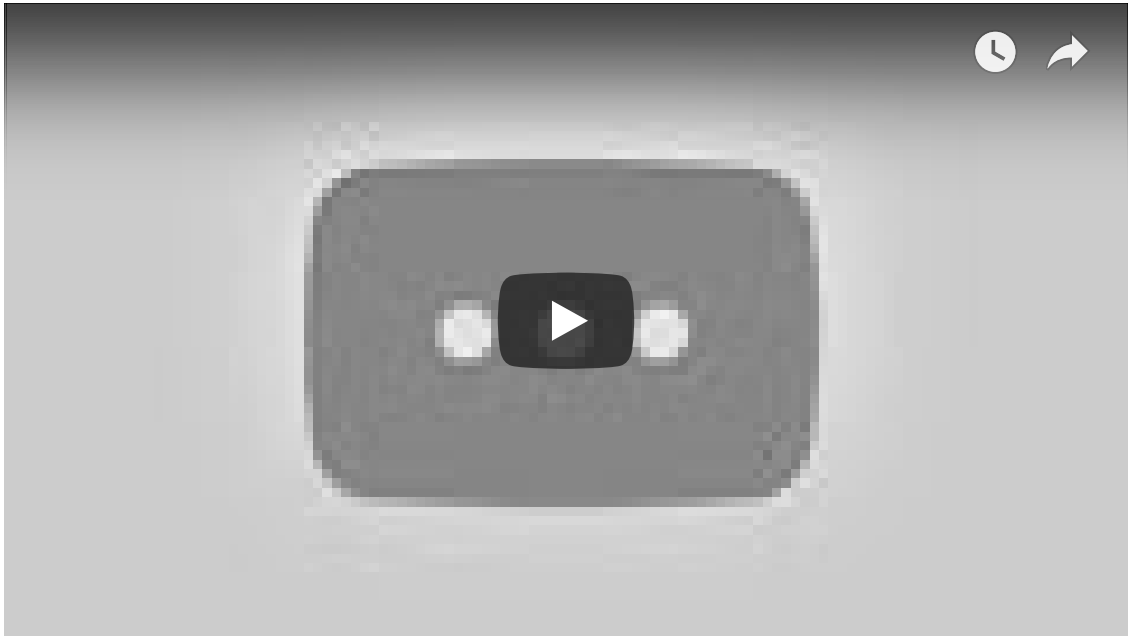
PrivEsc: Insecure Service Permissions

Published on January 3, 2016 By HollyGraceful on Build Security



I've written a few articles recently about methods of escalating privileges on Windows machines, such as through DLL Hijacking and Unquoted Service Paths, so here I'm continuing the series with Privilege Escalation through Insecure Service configurations. This one's pretty simple issue really, generally speaking it's simply a matter of altering the service so that it runs the executable and parameters you want it to, instead the default configuration allowing you to supply a command and privilege level for the execution. So you can simply run the add user command as local system and create your own local administrator account!

The first step in the detection is to find a service with weak permissions, this can be done with the accesschk tool from Sysinternals, which is available here.

You can execute the command as follows to list potentially vulnerable services:

```
accesschk.exe -uwcqv *
```

This will show list each service and the groups which have write permissions to that service – if you have an account in any of these groups then you've potentially got privilege escalation. If the output of the above command is a little too much to dig through, you could instead supply a group and it will limit output to services that group has write permission to, as:

```
accesschk.exe -uwcqv "Group Name" *
e.g.
accesschk.exe -uwcqv "Authenticated Users" *
accesschk.exe -uwcqv "Everyone" *
```

The output will be the service name, the group name and the permissions that group has. Anything like SERVICE_CHANGE_CONFIG or SERVICE_ALL_ACCESS is a win. In fact any of the following permissions are worth looking out for:

SERVICE_CHANGE_CONFIG
SERVICE_ALL_ACCESS
GENERIC_WRITE
GENERIC_ALL
WRITE_DAC
WRITE_OWNER

If you have reconfiguration permissions, or can get them through the above permission list, then you can use the SC command to exploit the vulnerability:

```
~~sc config SERVICENAME binpath= "net user hacker /add"~~
sc config SERVICENAME binPath= "E:\Service.exe"
sc config SERVICENAME obj=".LocalSystem" password=""
net stop SERVICENAME
net start SERVICENAME
```

Originally I posted that it was possible to set binPath directly to the *net user* command, although this seems to be a mistake on my part! The best way to achieve the same thing is to deploy an EXE which executes those commands and set binPath to that file. Also watch out for the space after the equals sign!

At this point you should find that you've successfully created a local user account on the target machine, change the binpath to add the user to the administrators group by setting it to the following command:

```
~~net localgroup "Administrators" hacker /add~~
```

Stop and start the service again and you're a Local Admin!

Remediation

The remediation for this one is fairly simple, lower privilege accounts such as domain users and their associated groups such as "Everyone" and "Authenticated Users" should not have any of the dangerous permissions listed above. The easiest thing to do, if possible,

is to remove any vulnerable services. However if that is not possible and the service's permission must be reconfigured then be warned that this isn't the simplest process. If you need to take these steps then take a look at Microsoft's guide: Best practices and guidance for writers of service discretionary access control lists...and maybe make a coffee before you get involved in the reconfiguration.

Tags: PrivEsc Privilege Escalation

Introduction to Burp Suite Pro

PrivEsc: DLL Hijacking

Theme Options

Default
Stereotype
Alternate
Beta

Tweets by @HollyGraceful

Tweets by @HollyGraceful

HollyGraceful Retweeted

FROVO
@fro_vo

POCAHONTAS: ♫ can you paint with all the colors of the wind ♫

ME: *literally wrestling neil degrasse tyson to the ground* jus- just let her sing neil

4 May 2018

HollyGraceful
@HollyGraceful

Lying in the tattoo place again; hopefully only a few more hours and then the whole piece will be done!

8 May 2018

HollyGraceful
@HollyGraceful

Replying to @HollyGraceful

“Holly, you can’t render 4K footage on a MacBook Air from 2013.”
“WHAT?!”
“I SAID YOU CAN’T RENDER 4K FOOTAGE IN 2013!”

Embed View on Twitter