n2dez / Rapid7-Insight-Agent-runas.md Secret

Created 11 months ago

☆ Star

<> Code -o- Revisions 1

Rapid7-Insight-Agent-runas.md

Privilege Escalation via Improper Quoting Path Vulnerability

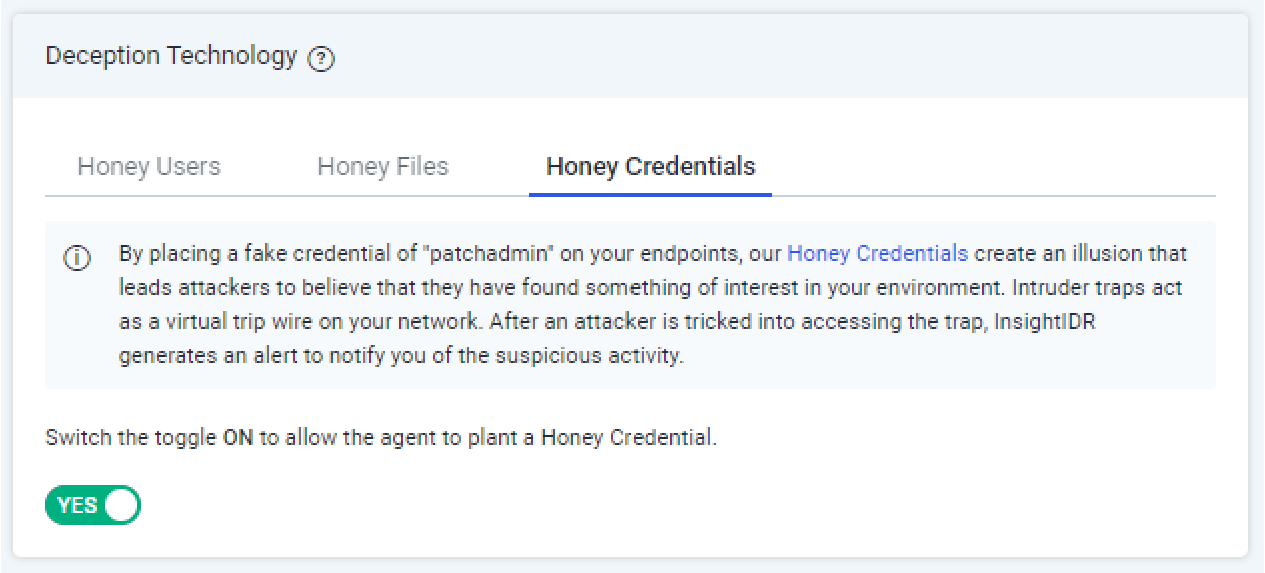
The Rapid7 Insight Agent v3.1.2.38 and earlier is not properly double-quoting with its use of runas, which allows a local adversary to execute code with system privileges.

Severity

7.8 HIGH

Analysis

1. Windows 10 with Insight Agent installed and 'Honey Credentials' enabled under 'Deception Technology' within InsightIDR



Deception Technology ?

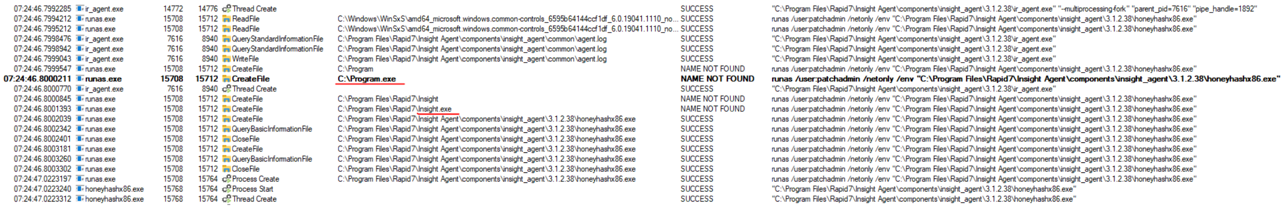
By placing a fake credential of "patchadmin" on your endpoints, our Honey Credentials create an illusion that leads attackers to believe that they have found something of interest in your environment. Intruder traps act as a virtual trip wire on your network. After an attacker is tricked into accessing the trap, InsightIDR generates an alert to notify you of the suspicious activity.

Switch the toggle **ON** to allow the agent to plant a Honey Credential.

YES

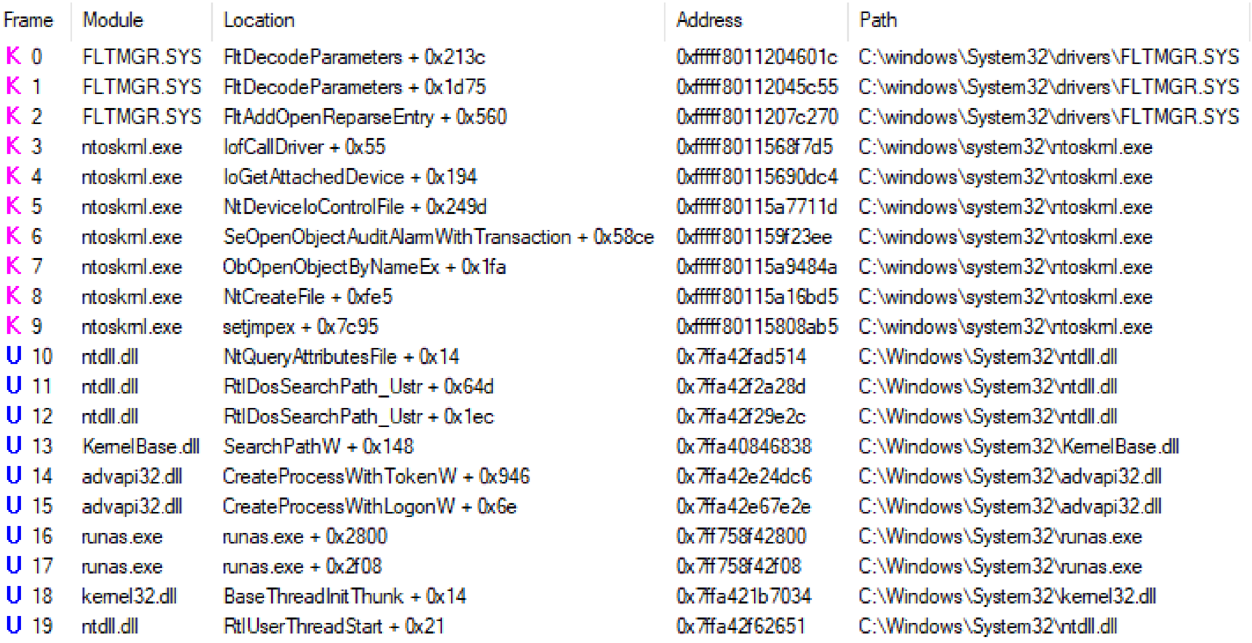
2. After a reboot, utilizing procmon boot-logging, we can see the call for 'Program.exe' via commandline utilizing Windows 'runas' only single-quoted

```
runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight
Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
```



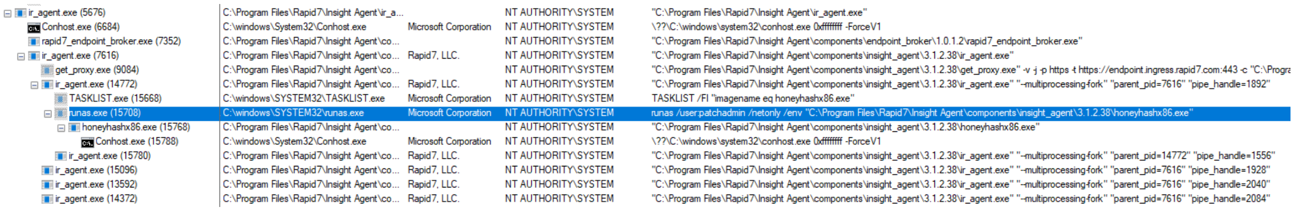
```
07:24:46.7992285  ir_agent.exe       14772  14776  Thread Create                                                                                                                SUCCESS          "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe" "--multiprocessing-fork" "parent_pid=7616" "pipe_handle=1892"
07:24:46.7994212  runas.exe          15708  15712  ReadFile                          C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.1110_no...   SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.7995212  runas.exe          15708  15712  ReadFile                          C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.1110_no...   SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.7998476  ir_agent.exe        7616   8940  QueryStandardInformationFile      C:\Program Files\Rapid7\Insight Agent\components\insight_agent\common\agent.log                   SUCCESS          "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe"
07:24:46.7998942  ir_agent.exe        7616   8940  QueryStandardInformationFile      C:\Program Files\Rapid7\Insight Agent\components\insight_agent\common\agent.log                   SUCCESS          "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe"
07:24:46.7999043  ir_agent.exe        7616   8940  WriteFile                         C:\Program Files\Rapid7\Insight Agent\components\insight_agent\common\agent.log                   SUCCESS          "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe"
07:24:46.7999547  runas.exe          15708  15712  CreateFile                        C:\Program                                                                                        NAME NOT FOUND   runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8000211  runas.exe          15708  15712  CreateFile                        C:\Program.exe                                                                                    NAME NOT FOUND   runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8000770  ir_agent.exe        7616   8940  Thread Create                                                                                                                SUCCESS          "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe"
07:24:46.8000845  runas.exe          15708  15712  CreateFile                        C:\Program Files\Rapid7\Insight                                                                   NAME NOT FOUND   runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8001393  runas.exe          15708  15712  CreateFile                        C:\Program Files\Rapid7\Insight.exe                                                               NAME NOT FOUND   runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8002039  runas.exe          15708  15712  CreateFile                        C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe          SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8002342  runas.exe          15708  15712  QueryBasicInformationFile         C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe          SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8002401  runas.exe          15708  15712  CloseFile                         C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe          SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8003181  runas.exe          15708  15712  CreateFile                        C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe          SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8003260  runas.exe          15708  15712  QueryBasicInformationFile         C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe          SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:46.8003302  runas.exe          15708  15712  CloseFile                         C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe          SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:47.0223197  runas.exe          15708  15764  Process Create                    C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe          SUCCESS          runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:47.0223240  honeyhashx86.exe   15768  15764  Process Start                                                                                                                SUCCESS          "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
07:24:47.0223312  honeyhashx86.exe   15768  15764  Thread Create                                                                                                                SUCCESS          "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
```

3. The stack trace for this call can be seen here



Frame	Module	Location	Address	Path
K 0	FLTMGR.SYS	FltDecodeParameters + 0x213c	0xfffff8011204601c	C:\windows\System32\drivers\FLTMGR.SYS
K 1	FLTMGR.SYS	FltDecodeParameters + 0x1d75	0xfffff80112045c55	C:\windows\System32\drivers\FLTMGR.SYS
K 2	FLTMGR.SYS	FltAddOpenReparseEntry + 0x560	0xfffff8011207c270	C:\windows\System32\drivers\FLTMGR.SYS
K 3	ntoskrnl.exe	IofCallDriver + 0x55	0xfffff8011568f7d5	C:\windows\system32\ntoskrnl.exe
K 4	ntoskrnl.exe	IoGetAttachedDevice + 0x194	0xfffff80115690dc4	C:\windows\system32\ntoskrnl.exe
K 5	ntoskrnl.exe	NtDeviceIoControlFile + 0x249d	0xfffff80115a7711d	C:\windows\system32\ntoskrnl.exe
K 6	ntoskrnl.exe	SeOpenObjectAuditAlarmWithTransaction + 0x58ce	0xfffff801159f23ee	C:\windows\system32\ntoskrnl.exe
K 7	ntoskrnl.exe	ObOpenObjectByNameEx + 0x1fa	0xfffff80115a9484a	C:\windows\system32\ntoskrnl.exe
K 8	ntoskrnl.exe	NtCreateFile + 0xfe5	0xfffff80115a16bd5	C:\windows\system32\ntoskrnl.exe
K 9	ntoskrnl.exe	setjmpex + 0x7c95	0xfffff80115808ab5	C:\windows\system32\ntoskrnl.exe
U 10	ntdll.dll	NtQueryAttributesFile + 0x14	0x7ffa42fad514	C:\Windows\System32\ntdll.dll
U 11	ntdll.dll	RtlDosSearchPath_Ustr + 0x64d	0x7ffa42f2a28d	C:\Windows\System32\ntdll.dll
U 12	ntdll.dll	RtlDosSearchPath_Ustr + 0x1ec	0x7ffa42f29e2c	C:\Windows\System32\ntdll.dll
U 13	KernelBase.dll	SearchPathW + 0x148	0x7ffa40846838	C:\Windows\System32\KernelBase.dll
U 14	advapi32.dll	CreateProcessWithTokenW + 0x946	0x7ffa42e24dc6	C:\Windows\System32\advapi32.dll
U 15	advapi32.dll	CreateProcessWithLogonW + 0x6e	0x7ffa42e67e2e	C:\Windows\System32\advapi32.dll
U 16	runas.exe	runas.exe + 0x2800	0x7ff758f42800	C:\Windows\System32\runas.exe
U 17	runas.exe	runas.exe + 0x2f08	0x7ff758f42f08	C:\Windows\System32\runas.exe
U 18	kernel32.dll	BaseThreadInitThunk + 0x14	0x7ffa421b7034	C:\Windows\System32\kernel32.dll
U 19	ntdll.dll	RtlUserThreadStart + 0x21	0x7ffa42f62651	C:\Windows\System32\ntdll.dll

4. Along with process tree outlining it's running with SYSTEM privileges



⊟ ir_agent.exe (5676)	C:\Program Files\Rapid7\Insight Agent\ir_a...		NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\ir_agent.exe"
Conhost.exe (6684)	C:\windows\System32\Conhost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1
rapid7_endpoint_broker.exe (7352)	C:\Program Files\Rapid7\Insight Agent\co...		NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\endpoint_broker\1.0.1.2\rapid7_endpoint_broker.exe"
⊟ ir_agent.exe (7616)	C:\Program Files\Rapid7\Insight Agent\co...	Rapid7, LLC.	NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe"
get_proxy.exe (9084)	C:\Program Files\Rapid7\Insight Agent\co...		NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\get_proxy.exe" -v -j -p https -t https://endpoint.ingress.rapid7.com:443 -c "C:\Progra
⊟ ir_agent.exe (14772)	C:\Program Files\Rapid7\Insight Agent\co...	Rapid7, LLC.	NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe" "--multiprocessing-fork" "parent_pid=7616" "pipe_handle=1892"
TASKLIST.exe (15668)	C:\windows\SYSTEM32\TASKLIST.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	TASKLIST /FI "imagename eq honeyhashx86.exe"
⊟ runas.exe (15708)	C:\windows\SYSTEM32\runas.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	runas /user:patchadmin /netonly /env "C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
⊟ honeyhashx86.exe (15768)	C:\Program Files\Rapid7\Insight Agent\co...		NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe"
Conhost.exe (15788)	C:\windows\System32\Conhost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1
ir_agent.exe (15780)	C:\Program Files\Rapid7\Insight Agent\co...	Rapid7, LLC.	NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe" "--multiprocessing-fork" "parent_pid=14772" "pipe_handle=1556"
ir_agent.exe (15096)	C:\Program Files\Rapid7\Insight Agent\co...	Rapid7, LLC.	NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe" "--multiprocessing-fork" "parent_pid=7616" "pipe_handle=1928"
ir_agent.exe (13592)	C:\Program Files\Rapid7\Insight Agent\co...	Rapid7, LLC.	NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe" "--multiprocessing-fork" "parent_pid=7616" "pipe_handle=2040"
ir_agent.exe (14372)	C:\Program Files\Rapid7\Insight Agent\co...	Rapid7, LLC.	NT AUTHORITY\SYSTEM	"C:\Program Files\Rapid7\Insight Agent\components\insight_agent\3.1.2.38\ir_agent.exe" "--multiprocessing-fork" "parent_pid=7616" "pipe_handle=2084"

Exploit

This can be exploited by creating the file 'c:\Program.exe' which would then be picked up by 'ir_agent.exe' invoked call to 'runas'. This would be called after every reboot.

Improper quoting allows for external modules to be called instead of intended module due to spaces within the path. This call is done with SYSTEM level privileges and attacker module would obtain this privilege when called. One can not assume all paths have been secured outside of application controlled directory.

More information on the topic:

- MITRE ATT&CK ID:T1574.009 [https://attack.mitre.org/techniques/T1574/009/]
- CWE-428: Unquoted Search Path or Element [https://cwe.mitre.org/data/definitions/428.html]
- Microsoft API: CreateProcessWithTokenW [https://docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-createprocesswithtokenw]

Fix

Windows runas when used with spaces in the path needs to be double-quoted.

```
runas /user:patchadmin /netonly /env "\"C:\Program Files\Rapid7\Insight
Agent\components\insight_agent\3.1.2.38\honeyhashx86.exe\""
```

Timeline

20220114 - initial disclosure to Rapid7