SCX RunAsProvider ExecuteShellCommand #3059

New issue

Merged shainw merged 4 commits into `Azure:master` from `Cyb3rWard0g:master` on Sep 17, 2021

Conversation 5 Commits 4 Checks 0 Files changed 1 +43 −0

Cyb3rWard0g commented on Sep 17, 2021 • edited Contributor

This hunting query uses Auditd security events collected via the Syslog data connector to explore the use of the SCX RunAsProvider Invoke_ExecuteShellCommand to execute any UNIX/Linux command using the /bin/sh shell.

SCXcore, started as the Microsoft Operations Manager UNIX/Linux Agent, is now used in a host of products including Microsoft Operations Manager. Microsoft Azure, and Microsoft Operations Management Suite.

SCX has a support provider named RunAsProvider. This provider has a few classes:

- ExecuteCommand
- ExecuteShellCommand
- ExecuteScript

Based on OMIGOD: Critical Vulnerabilities in OMI Affecting Countless Azure Customers by Wiz , `ExecuteShellCommand` was used in the HTTP request to test `CVE-2021-38647`.

```
<s:Body>
      <p:ExecuteShellCommand_INPUT xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/
         <p:command>id</p:command>
         <p:timeout>0</p:timeout>
      </p:ExecuteShellCommand_INPUT>
   </s:Body>
```

This was derived from initial testing while executing commands via `/opt/omi/bin/omicli` and exploring responses.

```
/opt/omi/bin/omicli --hostname 192.168.1.1 -u azureuser -p Password1 iv roo
```

Using the same template provided in the blog post by Wiz, we prepared a quick test:

```
<s:Body>
      <p:ExecuteShellCommand_INPUT xmlns:p="http://schemas.dmtf.org/wbem/wscim/1/
         <p:command>echo 'Hola MSTIC'</p:command>
         <p:timeout>0</p:timeout>
      </p:ExecuteShellCommand_INPUT>
   </s:Body>
```

We set the SCX logging to `verbose`

```
/opt/microsoft/scx/bin/tools/scxadmin -log-set all verbose
```

and we were able to capture the activity on the OMI server side in the `scx.log`:

```
tail -f /var/opt/microsoft/scx/log/scx.log
```

Reviewers

- shainw ✓
- Amitbergman ●
- aprakash13 ●
- ashwin-patil ●
- dicolanl ●
- ianhelle ●
- juliango2100 ●
- laithhisham ●
- liatlishams ●
- liemilyg ●
- lior-tamir ●
- mgladi ●
- nazang ●
- NoamLandress ●
- oshezaf ●
- oshvartz ●
- petebryan ●
- preetikr ●
- sagamzu ●
- sarah-yo ●
- shschwar ●
- sreedharande ●
- timbMSFT ●
- Yaniv-Shasha ●
- YaronFruchtmann ●
- YuvalNaor ●

Assignees

No one assigned

Labels

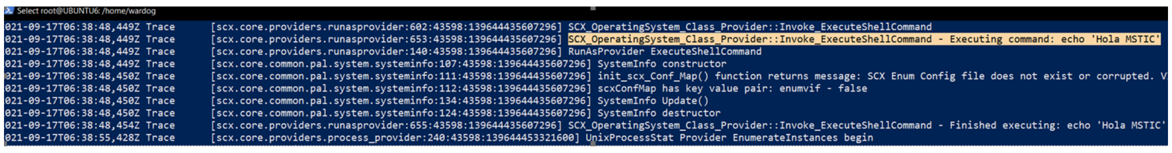
None yet

Projects

None yet

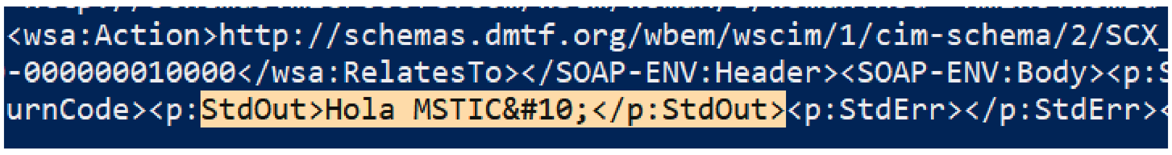
Milestone

No milestone



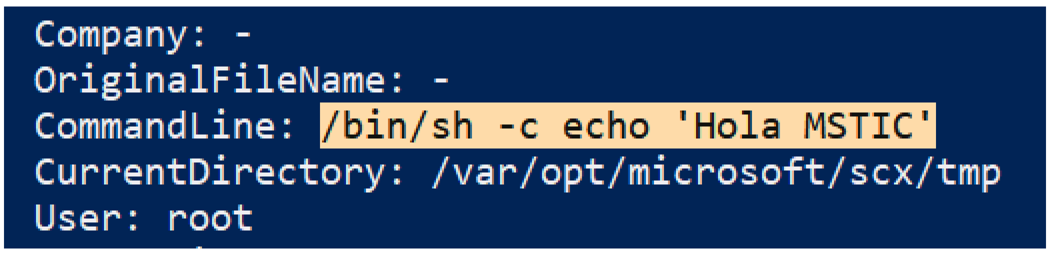
Select root@UBUNTU6: /home/wardog

```
021-09-17T06:38:48,449Z Trace      [scx.core.providers.runasprovider:602:43598:139644435607296] SCX_OperatingSystem_Class_Provider::Invoke_ExecuteShellCommand
021-09-17T06:38:48,449Z Trace      [scx.core.providers.runasprovider:653:43598:139644435607296] SCX_OperatingSystem_Class_Provider::Invoke_ExecuteShellCommand - Executing command: echo 'Hola MSTIC'
021-09-17T06:38:48,449Z Trace      [scx.core.providers.runasprovider:140:43598:139644435607296] RunAsProvider ExecuteShellCommand
021-09-17T06:38:48,449Z Trace      [scx.core.common.pal.system.systeminfo:107:43598:139644435607296] SystemInfo constructor
021-09-17T06:38:48,450Z Trace      [scx.core.common.pal.system.systeminfo:111:43598:139644435607296] init_scx_Conf_Map() function returns message: SCX Enum Config file does not exist or corrupted. V
021-09-17T06:38:48,450Z Trace      [scx.core.common.pal.system.systeminfo:112:43598:139644435607296] scxConfMap has key value pair: enumvif - false
021-09-17T06:38:48,450Z Trace      [scx.core.common.pal.system.systeminfo:134:43598:139644435607296] SystemInfo Update()
021-09-17T06:38:48,450Z Trace      [scx.core.common.pal.system.systeminfo:124:43598:139644435607296] SystemInfo destructor
021-09-17T06:38:48,454Z Trace      [scx.core.providers.runasprovider:655:43598:139644435607296] SCX_OperatingSystem_Class_Provider::Invoke_ExecuteShellCommand - Finished executing: echo 'Hola MSTIC'
021-09-17T06:38:55,428Z Trace      [scx.core.providers.process_provider:240:43598:139644453321600] UnixProcessStat Provider EnumerateInstances begin
```

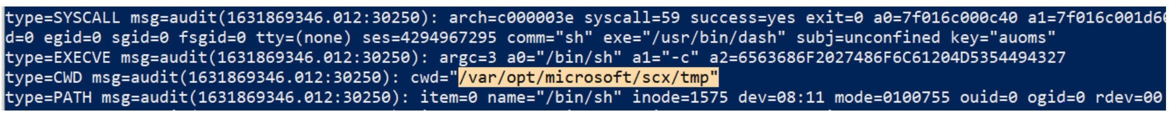


```
<wsa:Action>http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/SCX_
-000000010000</wsa:RelatesTo></SOAP-ENV:Header><SOAP-ENV:Body><p:S
urnCode><p:StdOut>Hola MSTIC&#10;</p:StdOut><p:StdErr></p:StdErr><
```

Next, we checked our `Sysmon for Linux` and `auditd` logs in our lab environment and identified where the commands were being executed from:

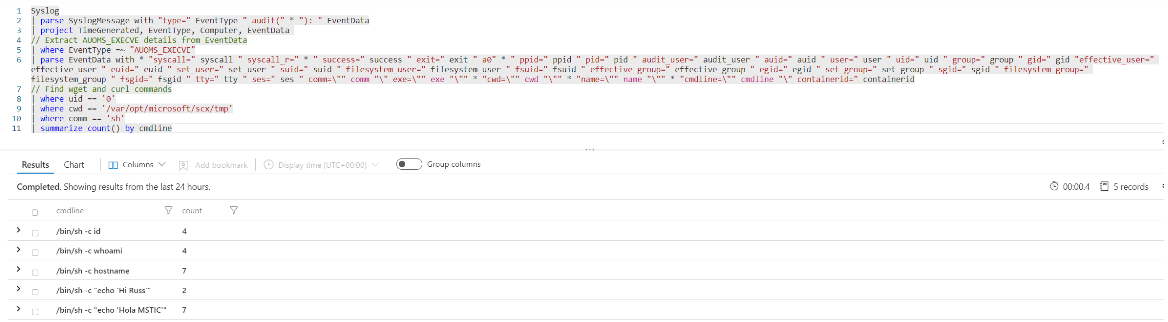


```
Company: -
OriginalFileName: -
CommandLine: /bin/sh -c echo 'Hola MSTIC'
CurrentDirectory: /var/opt/microsoft/scx/tmp
User: root
```



```
type=SYSCALL msg=audit(1631869346.012:30250): arch=c000003e syscall=59 success=yes exit=0 a0=7f016c000c40 a1=7f016c001d6
d=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="sh" exe="/usr/bin/dash" subj=unconfined key="auoms"
type=EXECVE msg=audit(1631869346.012:30250): argc=3 a0="/bin/sh" a1="-c" a2=6563686F2027486F6C61204D5354494327
type=CWD msg=audit(1631869346.012:30250): cwd="/var/opt/microsoft/scx/tmp"
type=PATH msg=audit(1631869346.012:30250): item=0 name="/bin/sh" inode=1575 dev=08:11 mode=0100755 ouid=0 ogid=0 rdev=00
```

We then put together the following query to validate our testing. The query is part of this PR.



```
Syslog
| parse SyslogMessage with "type=" EventType " audit(" * "): " EventData
| project TimeGenerated, EventType, Computer, EventData
// Extract AUOMS_EXECVE details from EventData
| where EventType =~ "AUOMS_EXECVE"
| parse EventData with * "syscall=" syscall " syscall_r=" * " success=" success " exit=" exit " a0" * " ppid=" ppid " pid=" pid " audit_user=" audit_user " auid=" auid " user=" user " uid=" uid " group=" group " gid=" gid "effective_user=" effective_user " euid=" euid " set_user=" set_user " suid=" suid " filesystem_user=" filesystem_user " fsuid=" fsuid " effective_group=" effective_group " egid=" egid " set_group=" set_group " sgid=" sgid " filesystem_group=" filesystem_group " fsgid=" fsgid " tty=" tty " ses=" ses " comm=\"" comm "\" exe=\"" exe "\"" * "cwd=\"" cwd "\"" * "name=\"" name "\"" * "cmdline=\"" cmdline "\" containerid=" containerid
// Find wget and curl commands
| where uid == '0'
| where cwd == '/var/opt/microsoft/scx/tmp'
| where comm == 'sh'
| summarize count() by cmdline
```

Completed. Showing results from the last 24 hours.

00:00.4 5 records

cmdline	count_
/bin/sh -c id	4
/bin/sh -c whoami	4
/bin/sh -c hostname	7
/bin/sh -c "echo 'Hi Russ'"	2
/bin/sh -c "echo 'Hola MSTIC'"	7

References:

- https://www.wiz.io/blog/omigod-critical-vulnerabilities-in-omi-azure
- https://docs.microsoft.com/en-us/system-center/scom/manage-security-administer-crossplat-agent?view=sc-om-2019
- https://github.com/microsoft/SCXcore
- https://github.com/microsoft/SCXcore/blob/master/source/code/providers/support/runasprovider.cpp#L137

Cyb3rWard0g added 3 commits 3 years ago

`New hunting query to explore the use of SCX RunAsProvider ExecuteShel…` ···	843255b
`Merge branch 'master' of https://github.com/Azure/Azure-Sentinel`	94c9e2d
`updated description of hunting query`	1ced1b3

Cyb3rWard0g requested review from **Amitbergman**, **aprakash13**, **ashwin-patil**, **dicolanl**, **ianhelle**, **juliango2100**, **laithhisham**, **liatlishams**, **liemilyg**, **lior-tamir**, **mgladi**, **nazang**, **NoamLandress**, **oshezaf**, **oshvartz**, **petebryan**, **preetikr**, **sagamzu**, **sarah-yo**, **shainw**, **shschwar**, **sreedharande**, **timbMSFT**, **Yaniv-Shasha**, **YaronFruchtmann** and **YuvalNaor** as code owners 3 years ago

shainw requested changes on Sep 17, 2021 **View reviewed changes**

shainw left a comment Contributor ···

1 recommended change and 1 potential change depending on what is in the user fields, otherwise good.

`Hunting Queries/Syslog/SCXRunAsProviderExecuteShellCommand.yml` Show resolved

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

`Hunting Queries/Syslog/SCXRunAsProviderExecuteShellCommand.yml` Show resolved

`added filter to improve performance and added Account entity type` `6289347`

✓ **shainw** approved these changes on Sep 17, 2021 View reviewed changes

shainw merged commit **`840bdb9`** into `Azure:master` on Sep 17, 2021

Sign up for free **to join this conversation on GitHub**. Already have an account? Sign in to comment