☰   🐙   **Sign in**

📘 **Azure** / **Azure-Sentinel**   Public

🔔 Notifications   ⑂ Fork **3k**   ☆ Star **4.6k**

<> Code   ⊙ Issues **26**   ⏸↻ Pull requests **82**   ▷ Actions   ⊞ Projects   📖 Wiki   ⚠ Security   〰 Insi

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 •   Contributor   • • •
edited ▾

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` .

Reviewers

❌ shainw   ✓

Amitbergman   ●

aprakash13   ●

ashwin-patil   ●

dicolanl   ●

ianhelle   ●

juliango2100   ●

laithhisham   ●

liatlishams   ●

liemilyg   ●

lior-tamir   ●

mgladi   ●

nazang   ●

NoamLandress   ●

oshezaf   ●

oshvartz   ●

(final)

```
<s:Body>
    <p:ExecuteShellCommand_INPUT xmlns:p="http://schem
        <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 azur
```

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

```
<s:Body>
    <p:ExecuteShellCommand_INPUT xmlns:p="http://schem
        <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
```

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
```


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

Sidebar

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

Development
Successfully merging this pull request may close these issues.
None yet

2 participants

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=7f016c001d60
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.

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/SCXRunAsProv          ⇕ Show resolved
iderExecuteShellCommand.yml
```

```
Hunting Queries/Syslog/SCXRunAsProv          ⇕ Show resolved
iderExecuteShellCommand.yml
```

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

shainw approved these changes on Sep 17, 2021

View reviewed changes

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

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

© 2024 GitHub, Inc.