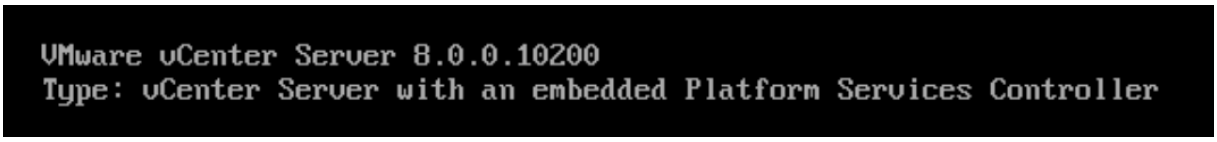
VMware vCenter Disclosures

Version 8.0.0.10200

Environment:

- VMware vCenter 8.0.0.10200
- Photon Linux



Findings:

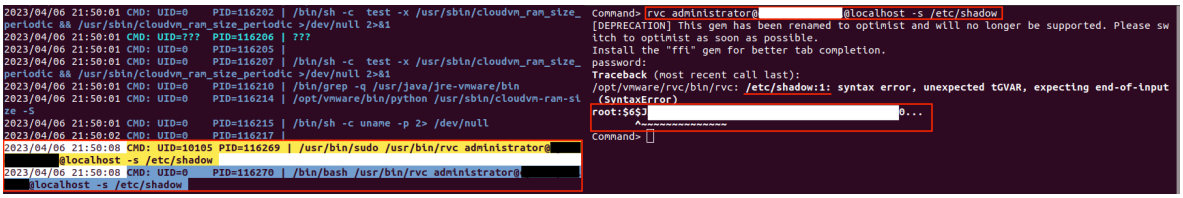
1. CVE-2024-22275: VMware vCenter Server Partial File Read

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”.

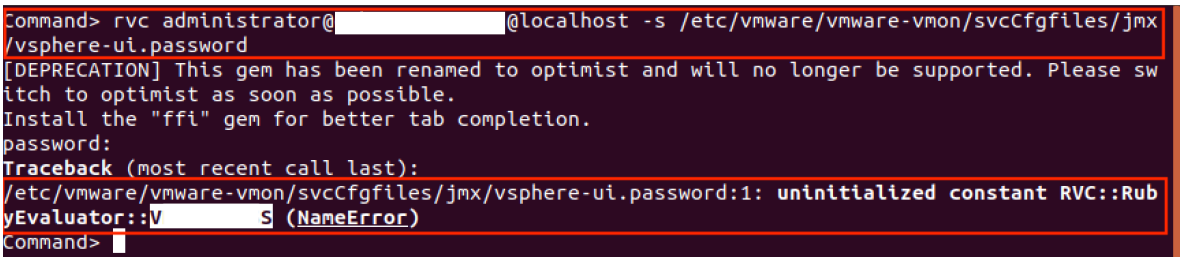
Because the binary runs as “root”, we can use the otherwise benign “-s” flag in order to read arbitrary files on the system as the “root” user to extract partial file contents via verbose errors.

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.

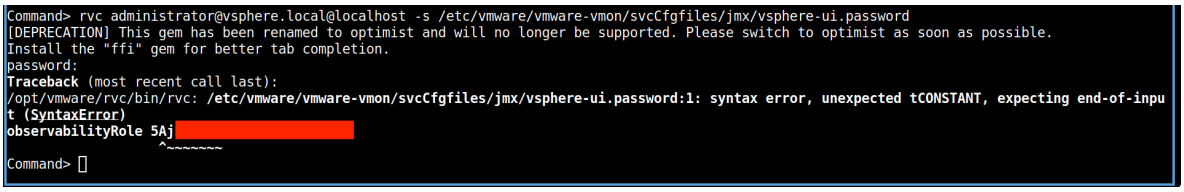


[1] https://github.com/DominicBreuker/pspy

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.



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



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.