Incident Report: CISA AA22-138B VMWare Workspace (Alt)

Summary:

This report details an alternative attack method used to exploit vulnerabilities in VMWare Workspace ONE Access, as described in the CISA alert AA22-138B. The attack involves the use of a malicious Bash script to exploit software vulnerabilities, escalate privileges, and establish command and control on the compromised system.

Attack Details:

The attackers initially exploited a vulnerability in VMWare Workspace ONE Access, specifically CVE 2022-22960, using a Bash script. This script allowed the attackers to escalate the privileges of a Horizon user, granting them the ability to execute commands and scripts with superuser (sudo) permissions.

Once the attackers gained elevated privileges, they used the Bash script to perform discovery on the compromised host, collecting network information and additional details about the system. To cover their tracks, the attackers overwrote the publishCaCert.hzn file with a file named fd86ald0.pem, effectively removing indicators of their presence.

The Bash script then proceeded to compress files containing sensitive information, such as network interface configurations, user credentials, master keys, hosts, and domains, into a TAR archive. This archive was stored in a specific VMWare Workspace ONE Access directory: /opt/vmware/horizon/workspace/webapps/SAAS/horizon/images/.

Using the compromised system, the attackers established command and control communication with the IP address 20.232.97.189. They attempted to download additional malicious tools, including a MoneroOcean cryptocurrency miner from GitHub, using the IP address 194.31.98.141.

Furthermore, the attackers used the IP address 8.45.41.114 to perform file and directory discovery, specifically targeting the /usr/local/horizon/conf directory. They also attempted to download a JSP webshell from the URL http://84.38.133[.]149/img/icon.gif.

The following additional IP addresses were observed downloading, executing, and checking the malicious Bash script:

- 45.72.112.245
- 115.167.53.141
- 191.102.179.197
- 209.127.110.126
- 45.72.85.172
- 192.241.67.12