Workaround Instructions for CVE-2021-22005

Article ID: 322789 Updated On: 10-28-2024

Products

VMware vCenter Server

Issue/Introduction

VMware has investigated CVE-2021-22005 and determined that the possibility of exploitation can be removed by performing the steps detailed in the **Workaround** section of this article.

This workaround is meant to be a temporary solution until updates documented in VMSA-2021-0020 can be deployed.

VCSA systems running version **7.0U2c** build **18356314** which was released on August 24th, and VCSA systems running version **6.7U3o** build **18485166** which was released on September 21st, are not vulnerable to this issue and this workaround is not required to be implemented on appliances running these versions.
All previous versions of 6.7 and 7.0 are vulnerable.
This workaround also applies to VCSAs running as external PSCs in a vCenter 6.7 environment
vCenter 6.5 versions are not exposed to this CVE and this workaround does not apply to any 6.5 VCSA
For customers running VCF, the workaround is required to be applied to all the vCenter systems running in your environment -- in both the management and all workload domains.

Resolution

Resolution for CVE-2021-22005 is documented in VMSA-2021-0020.

Workaround:

To implement the workaround for CVE-2021-22005 **on Linux-based virtual appliances (vCSA) perform the following steps:**

6.7 vCenters running on Windows are not impacted by CVE-2021-22005
There is no requirement to implement this workaround on 6.7 Windows VC systems
This workaround also applies

This workaround requires an
The update to the file involve

The required changes depen
For 6.7 U1b (Build 11726888)

For 6.7U2 (Build 13010631) ar
"phPhStgApiServlet" endpoin

Option 1 - Implement Workaround Via The "VMSA-2021-0020" Script

This script is provided to help customers implement the documented workaround in a timely and automated way
The script should **ONLY** be executed on **vulnerable** vCenter and PSC appliances
If you have patched or updated your systems to the fixed versions of either 6.7U3o or 70U2c, **please do not execute the script**. The endpoints have been updated in these versions and will return a "HTTP/1.1 400" status when the curl command documented at the end of the manuals steps is executed. See "Related Information" section below for more information

(Edit: Latest version of script not attached. This will report an "Environment is already patched for VMSA-2021-0020." message when executed on a patched system)

To use this approach, you must download the VMSA-2021-0020.py file attached to this article.
Then, use the file-moving utility of your choice (WinSCP for example) to copy the file to the appliance on which you wish to execute it.
The script will update the ph-web.xml file as required on ALL affected versions of 6.7 and 7.0.

NOTE: If you have troubles connecting to a vCenter appliance using WinSCP, please see Error when uploading files to vCenter Server Appliance using WinSCP

For the purposes on this document, the python script has been copied to the "**/var/tmp**" directory on the VCSA

Any directory can be used – but the location of the file will need to be updated in the commands below

Steps

1) Connect to the vCSA using an SSH session and root credentials

2) List the contents of the directory where you copied the file – to ensure it was copied successfully
In this case, that is "/var/tmp". Execute the command and ensure that the file is listed

```
ls -al /var/tmp/
```

3) Run the script by executing the command below
Change the path to the file as appropriate
The version of python to use depends on the exact version of your vCenter.
The script can be executed with python, python3.5 or python 3.7

```
python /var/tmp/VMSA-2021-0020.py
or
python3.5 /var/tmp/VMSA-2021-0020.py
or
python3.7 /var/tmp/VMSA-2021-0020.py
```

The script will execute and
a. Create a backup of the unmodified ph-web.xml
b. Update the ph-web.xml file
c. Create a backup of the updated ph-web.xml
d. Restart the analytics service
e. Confirm that the appliance is no longer vulnerable

See the output bellow (script executed with python 3.5 in this example)

```
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]# ls -al /var/tmp/
total 20
drwxrwxrwt  3 root root 4096 Sep 15 10:31 .
drwxr-xr-x 18 root root 4096 Apr 17  2018 ..
drwx------  3 root root 4096 Sep 13 14:40 systemd-private-ef11b61a673d4d08894e6b3dd7f4dd07-systemd-timesyncd.service-FNOZUL
-rw-r--r--  1 root root 6824 Sep 13 16:07 VMSA-2021-0020.py
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]# python3.5 /var/tmp/VMSA-2021-0020.py
OK : RPM version : VMware-analytics-6.7.0-8016741.x86_64

OK : Run time stamp : 2021-Sep-15-10-32-13

Checking for open vulnerabilities :
TEST : Push telemetry : < HTTP/1.1 201
WARNING : Vulnerability found.

Backing up the config file : /etc/vmware-analytics/ph-web.xml
OK : Config file backed up as : /var/log/vmware/analytics/ph-web.xml---BEFORE_PATCH---VMware-analytics-6.7.0-8016741.x86_64-2021-Sep-15-10-32-13.backup


Patching the config file: /etc/vmware-analytics/ph-web.xml
OK : Patched config file backed up as : /var/log/vmware/analytics/ph-web.xml---AFTER_PATCH---VMware-analytics-6.7.0-8016741.x86_64-2021-Sep-15-10-32-13.backup
OK : Patched the config file.

Running the restart command : service-control --stop analytics && service-control --start analytics
OK : Restart command completed.

Checking for open vulnerabilities :
TEST : Push telemetry : < HTTP/1.1 404
TEST : Create data app agent : < HTTP/1.1 404
TEST Data app collect : < HTTP/1.1 404
OK : Vulnerabilities were NOT found!


SUCCESS : Patching completed. Vulnerabilities are NOT detected.
root@vcsa1 [ ~ ]#
```

This completes the "scripted workaround"

Option 2 -- Implement The Workaround Via Manual Steps

1) Connect to the vCSA using an SSH session and root credentials.

2) Backup the /etc/vmware-analytics/ph-web.xml file:

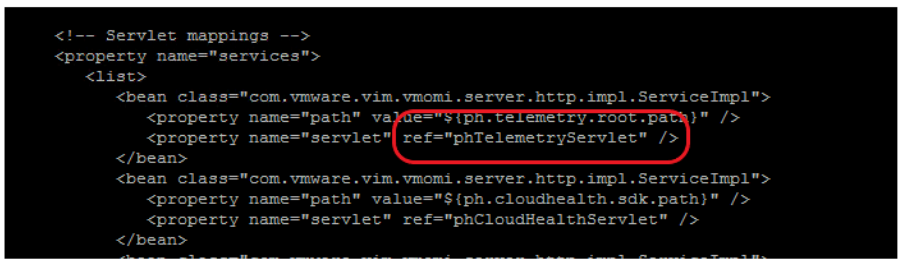
```
cp /etc/vmware-analytics/ph-web.xml /etc/vmware-analytics/ph-web.xml.backup
```

3) Open the /etc/vmware-analytics/ph-web.xml file in a text editor

```
vi /etc/vmware-analytics/ph-web.xml
```

4) Content of this file looks like below:

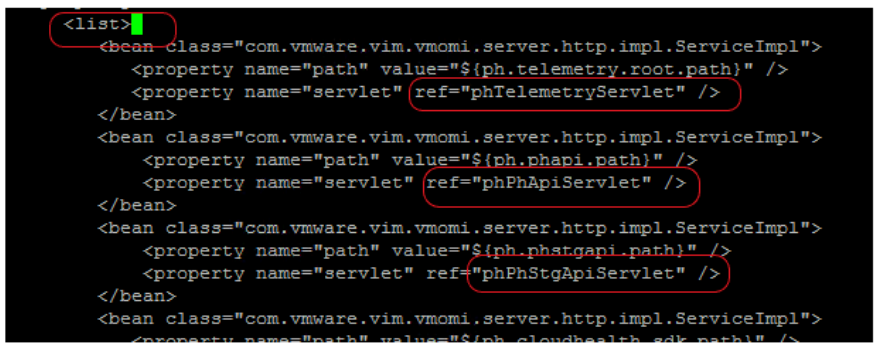
VCSA 6.7U2 (Build13010631) and later / VCSA7.0



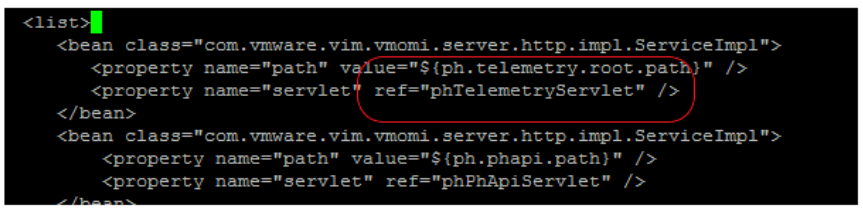
VCSA 6.7U1b (Build11726888) or earlier

5) Hit "**I**" on the keyboard to enter "**Insert**" mode (I for Insert)

6) Navigate to the "**<list>**" line as shown below



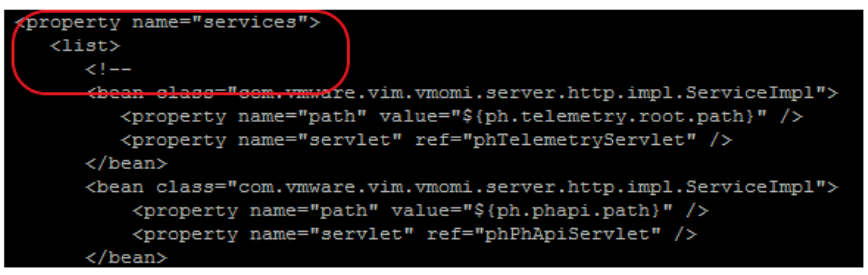
VCSA 6.7U2 (Build13010631) and later / VCSA7.0



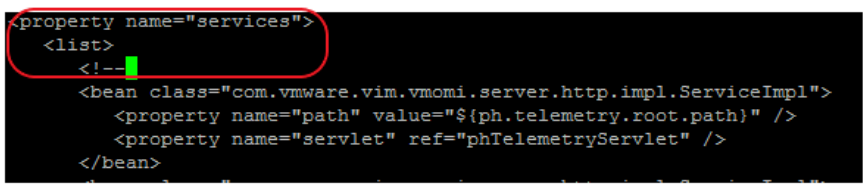
VCSA 6.7U1b (Build11726888) or earlier

7) Hit Enter

8) Type "**<!—**" as shown below



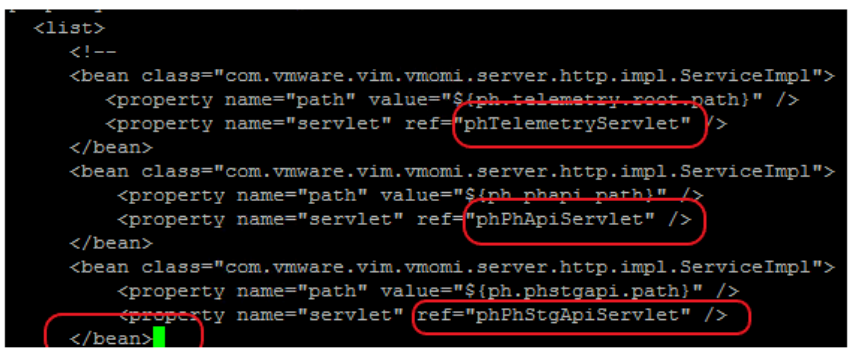
VCSA 6.7U2 (Build13010631) and later / VCSA7.0



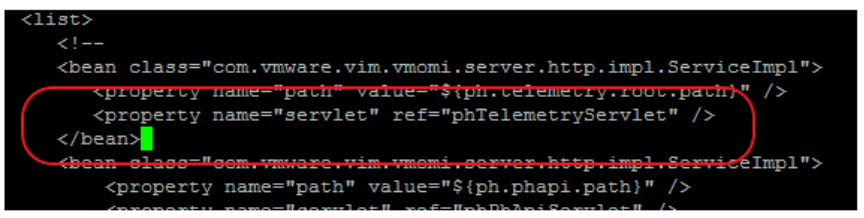
VCSA 6.7U1b (Build11726888) or earlier

9) Navigate to the "**</bean>**" line just after the "**<property name="servlet" ref="phPhStgApiServlet"/>**" line

On older versions of 6.7 (u1b or earlier) , you should navigate to the "**</bean>**" line just after the "**<property name="servlet" ref="phTelemetryServlet"/>**"

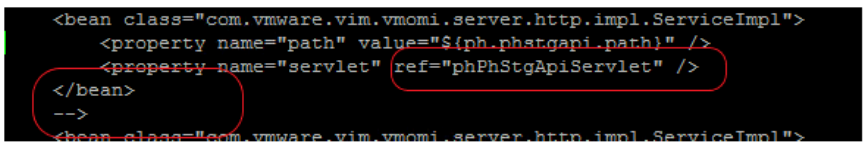


VCSA 6.7U2 (Build13010631) and later / VCSA7.0

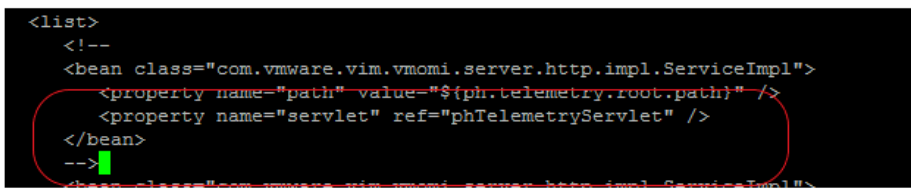


VCSA 6.7U1b (Build11726888) or earlier

10) Hit "**Enter**" and type "**-->**"



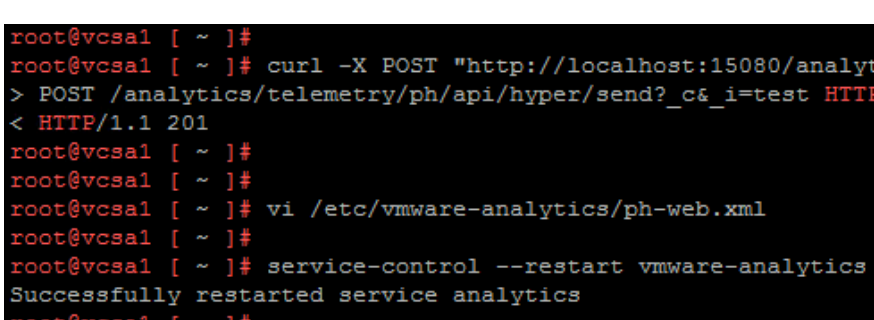
VCSA 6.7U2 (Build13010631) and later / VCSA7.0



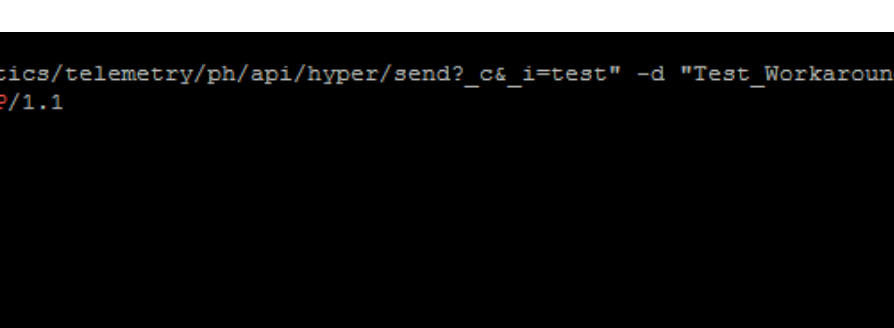
VCSA 6.7U1b (Build11726888) or earlier

11) Hit the "**Esc**" button on your keyboard to exit Insert mode

12) Save and exit the file by typing "**:wq**" and hitting "**Enter**"



VCSA 6.7U2 (Build13010631) and later / VCSA7.0



VCSA 6.7U1b (Build11726888) or earlier

13) Restart the vmware-analytics service by typing

service-control --restart vmware-analytics

14) To confirm that the workaround has taken effect, you can test by running the command below

curl -X POST "http://localhost:15080/analytics/telemetry/ph/api/hyper/send?_c&_i=test" -d "Test_Workaround" -H "Content-Type: application/json" -v 2>&1 | grep HTTP

This should return a 404 error

```
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]# curl -X POST "http://localhost:15080/analytics/telemetry/ph/api/hyper/send?_c&_i=test" -d "Test_Workaround"
> POST /analytics/telemetry/ph/api/hyper/send?_c&_i=test HTTP/1.1
< HTTP/1.1 201
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]# vi /etc/vmware-analytics/ph-web.xml
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]# service-control --restart vmware-analytics
Successfully restarted service analytics
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]# curl -X POST "http://localhost:15080/analytics/telemetry/ph/api/hyper/send?_c&_i=test" -d "Test_Workaround"
> POST /analytics/telemetry/ph/api/hyper/send?_c&_i=test HTTP/1.1
< HTTP/1.1 404
<!doctype html><html lang="en"><head><title>HTTP Status 404 – Not Found</title><style type="text/css">h1 {font-family:Tahoma,
olor:white;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#52
ily:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;co
der:none;}</style></head><body><h1>HTTP Status 404 – Not Found</h1><hr class="line" /><p><b>Type</b> Status Report</p><p><b>D
 to disclose that one exists.</p><hr class="line" /><h3>Apache Tomcat/8.5.40</h3></body></html>
root@vcsa1 [ ~ ]#
```

Additional Information

If the curl command docume
message will be returned

VCSA running 7.0U2d build 18

```
root@vcsa70 [ ~ ]# vpxd -v
VMware VirtualCenter 7.0.2 build-18455184
root@vcsa70 [ ~ ]#
root@vcsa70 [ ~ ]# curl -X POST "http://localhost:15080/analytics/telemetry/ph/api/hyper/send?_c&_i=test" -d "Test_Workaround" -H "Content-Type: application/json" -v 2>&1 | grep HTTP
> POST /analytics/telemetry/ph/api/hyper/send?_c&_i=test HTTP/1.1
< HTTP/1.1 400
root@vcsa70 [ ~ ]#
```

VCSA running 6.7U3o build 18485185

```
root@vcsa1 [ ~ ]# vpxd -v
VMware VirtualCenter 6.7.0 build-18485185
root@vcsa1 [ ~ ]#
root@vcsa1 [ ~ ]# curl -X POST "http://localhost:15080/analytics/telemetry/ph/api/hyper/send?_c&_i=test" -d "Test_Workaround" -H "Content-Type: application/json" -v 2>&1 | grep HTTP
> POST /analytics/telemetry/ph/api/hyper/send?_c&_i=test HTTP/1.1
< HTTP/1.1 400
root@vcsa1 [ ~ ]#
```

Impact/Risks:

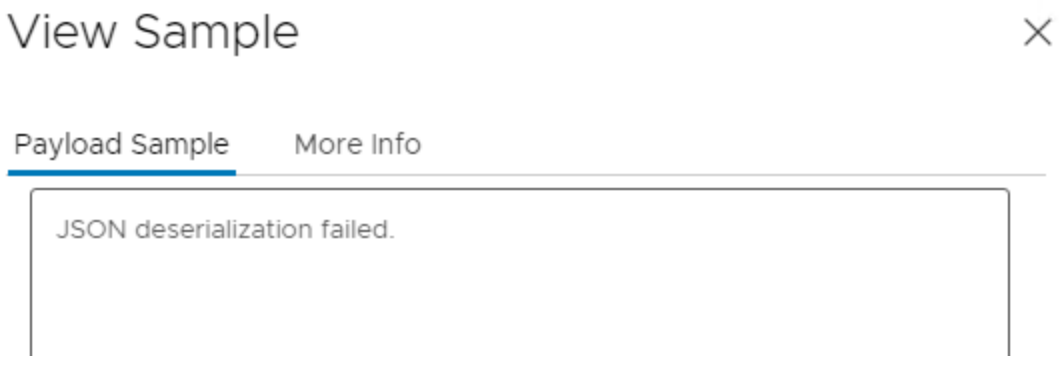
Functionality Impacts:
There is **no** functionality impact when the workaround is applied to a vCenter system running 6.7
On systems running 7.0. there is a very minor impact in that the user receives a “JSON deserialization failed” message when clicking on “Sample Data” under “Administration – Customer Experience Improvement Program”
This option is only available when CEIP is disabled

Implementing this workaround has no effect on any service that requires CEIP to be enabled such as

- Skyline Health For vSphere
- Skyline health For vSAN

In addition there is no impact on VMware Skyline Advisor.

The screenshot below shows the error received in 7.0 vCenters post implementing the workaround.
This can be safely ignored



Attachments

VMSA-2021-0020

Feedback

Was this article helpful?

Yes No