SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

Attackers Exploiting WebLogic Servers via CVE-2020-14882 to install Cobalt Strike

Published: 2020-11-03
Last Updated: 2020-11-04 13:50:55 UTC
by Renato Marinho (Version: 1)

Starting late last week, we observed a large number of scans against our WebLogic honeypots to detect if they are vulnerable to CVE-2020-14882. CVE-2020-14882 was patched about two weeks ago as part of Oracle's quarterly critical patch update. In addition to scans simply enumerating vulnerable servers, we saw a small number of scans starting on Friday (Oct. 30th) attempting to install crypto-mining tools [1].

On Friday, Oracle amended its patch for CVE-2020-14882 [2]. A new variation of the vulnerability (CVE-2020-14750) can be used to exploit WebLogic servers with a trivial modification of the exploit code.

Last Saturday we started seeing a campaign using a chain of Powershell obfuscated scripts to download a Cobalt Strike payload. According to Cisco Talos Q4 2020 CTIR report, 66% of all ransomware attacks this quarter involved the use of Cobalt Strike [3]. Thus, as expected, there is a high probability ransomware gang included CVE-2020-14882 exploit in their arsenal.

The attack, as seen in Figure 1, exploits the vulnerability to execute a PowerShell payload base64-encoded.

Figure 1 - Payload delivery

Decoding the base64 content, we can find the following code. As seen, there is another encoding layer using base64 and gzip compression. I usually make some adjustments to the original malicious script to make it save the decoded content to a file. So, replacing “IEX” by “$content =” and appending the script with “$content |out-file -filepath decoded_script.ps1” is enough to accomplish this result for this case.

Figure 2 - First stage decoding

Part of the resulting code is shown in Figure 3. Notice that there is another protected code. There is a loop decrypting each byte of the code using an XOR function with the byte 0x35.

Figure 3 - Second stage decoding

The result of this operation is a shellcode to download and execute a Cobalt Strike payload hosted at http://185[.]205.210.179:4321/Z8qZ.

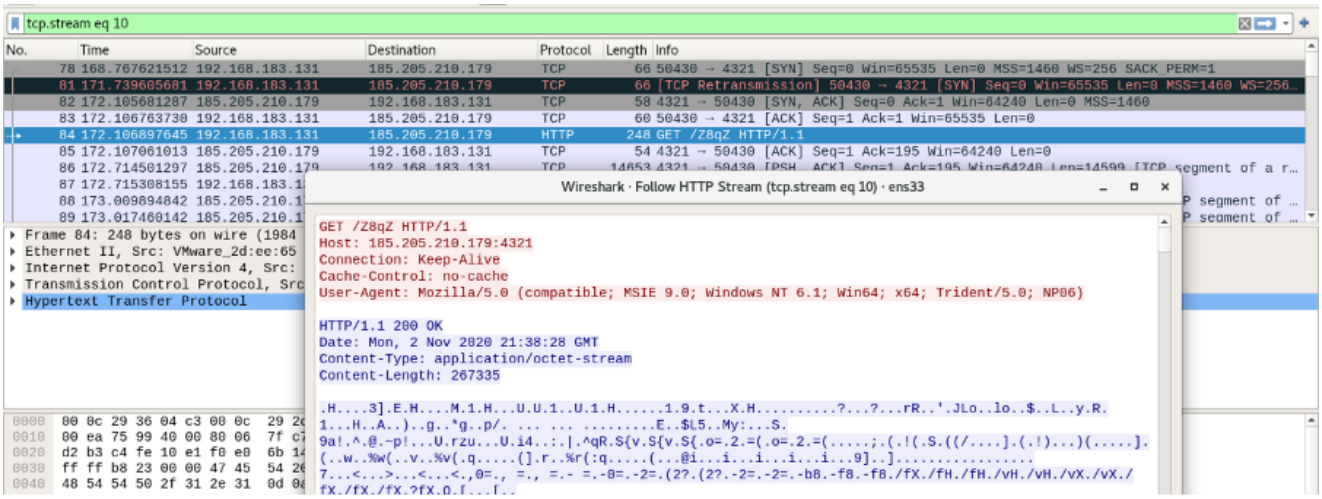
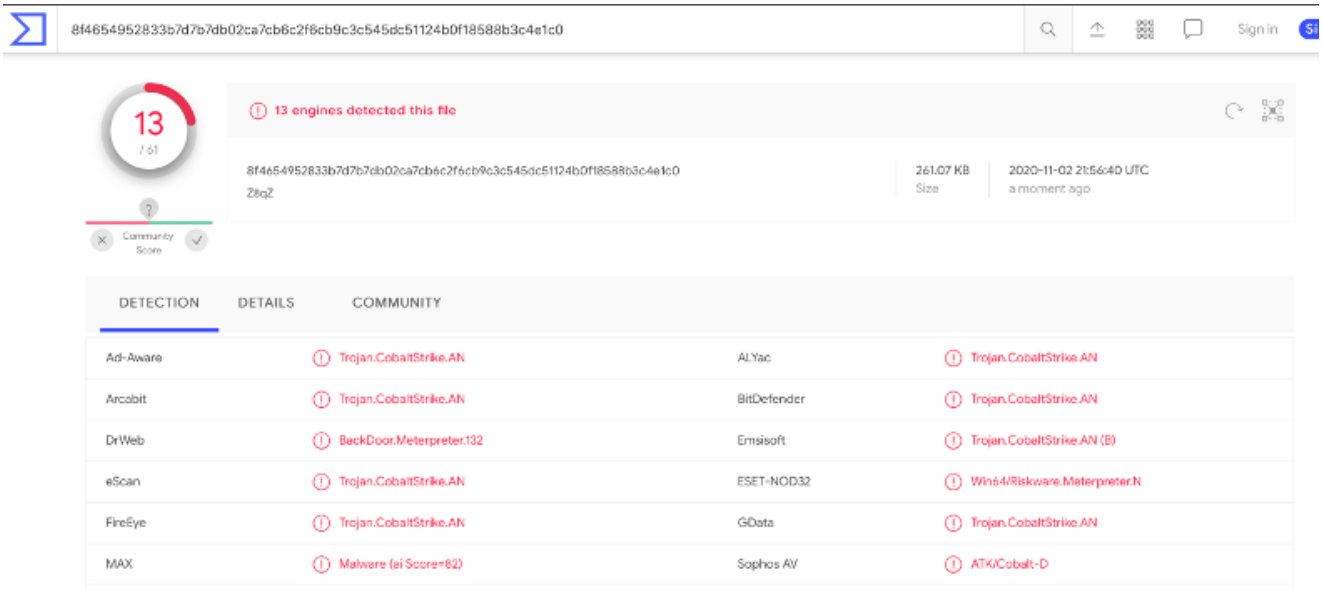


Figure 4 - Cobalt Strike payload download

Submitting the binary to VirusTotal, we had the following result:



]

Figure 5 - Cobalt Strike payload submitted to Virus Total

Running the malicious scripts in a controlled environment, it was possible to see connections established from time to time with the C2 at http://185[.]205.210.179/en_US/all.js.

References

[1] https://isc.sans.edu/forums/diary/PATCH+NOW+CVE202014882+Weblogic+Actively+Exploited+Against+Honeypots/26734/
[2] https://www.oracle.com/security-alerts/alert-cve-2020-14750.html#AppendixFMWl
[3] https://blog.talosintelligence.com/2020/09/CTIR-quarterly-trends-Q4-2020.html

IOCs:

Network:

45[.]134.26.174
http://185[.]205.210.179:4321/Z8qZ
http://185[.]205.210.179/en_US/all.js

Files:

Z8qZ:
8ca0251bc340fc207e6f832eb6165b8d (MD5)
8f4654952833b7d7b7db02ca7cb6c2f6cb9c3c545dc51124b0f18588b3c4e1c0 (SHA256)

The malicious requests are available at https://isc.sans.edu/WebLogicPS.log.zip

Keywords:

0 comment(s)

Top of page

×

Diary Archives

- Diary
- Podcasts
- Jobs
- Forums
  - Auditing
  - Diary Discussions
  - Forensics
  - General Discussions
  - Industry News
  - Network Security
  - Penetration Testing
  - Software Security
- SANS.edu Research