64

Remote Code Execution (RCE) in a DoD website

Share:

State	○ Resolved (Closed)
Disclosed	**October 4, 2019 8:51pm +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Code Injection
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

manoelt submitted a report to **U.S. Dept Of Defense**. Jul 11th (2 years ago)

Summary:
One of the DoD applications uses a java library which is vulnerable to expression language injection. Using only an URL I was able to inject java code. I made a simple PoC that requests a name resolution to a DNS server.

Description:
The application at https://[redacted] uses Primefaces version 5.3 which is vulnarable to Expression Language injection through DynamicContent generator.

To prove the injection I made a PoC that tries to submit a HTTP request, but the server blocks the outgoing packets on port 80, on the other hand the server still try to resolve the requested domain and so I receive DNS requests from DoD server. Also, I can delete and maybe read files using the File Java class, but I decided not to try to avoid leak of some private data.

Impact

Critical.

Step-by-step Reproduction Instructions

First you need to execute the program attached to generate the payload. To do that you just need the Primefaces-5.3.jar (https://www.primefaces.org/downloads/) in your class path.

1. With the code attached generate the payload encrypted with the default key "primefaces". Change the domain (String remoteMalJarUrl) to one that you have control or use one from http://dnsbin.zhack.ca/
2. With the payload from #1, append to the URL: https://[redacted]/javax.faces.resource/dynamiccontent.properties.xhtml?pfdrt=sc&ln=primefaces&pfdrid=
3. Send a GET request using curl (curl -vk https://[redacted]/javax.faces.resource/dynamiccontent.properties.xhtml?pfdrt=sc&ln=primefaces&pfdrid=<YOUR_PAYLOAD_HERE>
4. You will receive a name resolution request for remoteMalJarUrl from the DoD application

We could use this DNS request to exfiltrate data from the server. And as I said, theoretically I could also delete files from the server using the File class.

Product, Version, and Configuration (If applicable)

Primefaces 5.3

Suggested Mitigation/Remediation Actions

- Update Primefaces
- Alternatively by filtering incoming requests with pfdrid parameter (value longer than 16bytes and Base64 encoded) and "pfdrt=sc" is possible to mitigate the attack: "pfdrt=sc" calls the vulnerable StreamedContent Method and pfdrid contains the exploit payload.

References

http://blog.mindedsecurity.com/2016/02/rce-in-oracle-netbeans-opensource.html
https://github.com/primefaces/primefaces/issues/1152

BOT: U.S. Dept Of Defense posted a comment. Jul 11th (2 years ago)

Greetings from the Department of Defense (DoD),

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

opimentelsei updated the severity to Critical. Jul 13th (2 years ago)

opimentelsei changed the status to ○ **Triaged**. Jul 13th (2 years ago)

Greetings,

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

opimentelsei posted a comment. Sep 13th (2 years ago)

@manoelt

Greetings,

We have been advised that the vulnerability you reported has been resolved. Before we close this report, we would appreciate it if you could confirm that the vulnerability no longer exists.

If we do not receive a response within two weeks, we will send you a second request. If we do not receive a response from you within two weeks of the second notice, we will close this report as resolved.

If you do not believe this vulnerability has been effectively resolved or if you have any questions, please let us know.

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

Regards,

The VDP Team

opimentelsei posted a comment. Sep 27th (2 years ago)

@manoelt
Greetings,

We previously sent a request asking you to confirm that the vulnerability you reported has been resolved. We would like your confirmation before closing this report.

If we do not receive a response to this second request within two weeks, we will close this report as resolved.

If you do not believe this vulnerability has been effectively resolved or if you have any questions, please let us know.

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

Regards,

The VDP Team

manoelt posted a comment. Sep 30th (2 years ago)
@opimentelsei
I think it is fixed now. I can't reproduce anymore.

opimentelsei posted a comment. Oct 2nd (2 years ago)
@manoelt
How did you find out the version it was running?

manoelt posted a comment. Updated Sep 24th (17 days ago)
@opimentelsei
Just look at source code: view-source:https://[redacted]/users/forgotPassword.xhtml

You will see: <script type="text/javascript" src="/javax.faces.resource/jquery/jquery.js.xhtml?ln=primefaces&amp;v=6.0">

"v=6.0" is the Primefaces version.

opimentelsei closed the report and changed the status to ○ **Resolved**. Oct 4th (2 years ago)
Good news!

The vulnerability you reported is considered resolved and this report is now closed. If you have any questions, please let me know.

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

Regards,

The VDP Team

manoelt requested to disclose this report. Oct 4th (2 years ago)

manoelt posted a comment. Nov 21st (2 years ago)
@opimentelsei Could we disclose this report publicly?

manoelt posted a comment. Apr 18th (about 1 year ago)
Could we disclose this report publicly?

deez_nops posted a comment. Apr 18th (about 1 year ago)
@manoelt Unfortunately, not yet. We are in the final steps to standardize the disclosure process and working through the researchers requests, including your report. Thanks again for your patience.

manoelt posted a comment. Jun 26th (4 months ago)
Could we disclose this report publicly?

deez_nops posted a comment. Jun 26th (4 months ago)

@manoelt Right now we have an enourmous backlog of disclosures to process and, looking at the list, your's will probably be processed by sometime next week. Sorry for the huge delay but, your patience is appreciated.

ag3nt-j1 agreed to disclose this report. Oct 4th (7 days ago)

This report has been disclosed. Oct 4th (7 days ago)

U.S. Dept Of Defense has locked this report. Oct 4th (7 days ago)