IOActive.
Research-fueled Security Services

IOACTIVE CASE STUDY

Trivial Vulnerabilities, Big Risks

CNJ PJe

The Brazilian National Justice Council (CNJ) maintains a Judicial Data Processing System capable of facilitating the procedural activities of magistrates, judges, lawyers, and other participants in the Brazilian legal system with a single platform, making it ubiquitous as a result. The CNJ Processo Judicial Eletrônico (CNJ PJe) system processes judicial data, with the objective of fulfilling the needs of the organs of the Brazilian Judiciary Power[1]: Superior, Military, Labor, and Electoral courts; the courts of both the Federal Union and the individual states themselves; and the specialized justice systems that handle ordinary law and employment tribunals on both the federal and state level.

The CNJ PJeOffice[2] software allows access to a user's workspace through digital certificates, where individuals are provided with specific permissions, access controls, and scope of access in accordance with their roles. The primary purpose of this application is to guarantee legal authenticity and integrity to documents and processes through digital signatures.

The Challenge

In 2019, Brazilian lawyer João Falcão researched the possibility of retrieving and analysing process information from Brazilian state courts in a semi-automated manner. The goal was to gather decision insights[3], through probability and statistics, from 5,000 processes distributed across 10 different courts.

In an attempt to assist his research, it was suggested that he could use CNJ PJeOffice, as it provides a unified, common-access interface across multiple court systems—which led to the rapid discovery of the vulnerabilities found within the platform's update mechanism, during the very first round of tests.

Insecure communications between users and CNJ's infrastructure allowed an attacker to intercept and replace the original version of PJe's application with a modified version of their choice. After download, the installation process could be tampered with, bypassing authenticity and integrity validation of the software update, allowing the attacker's version to be installed instead.

Security Impact

The application's update system, which was found to be vulnerable to remote code execution, presented two immediate implications:

- Control of a victim's computer
- Control over PJe Office's user account, including all privileges that the user holds within the CNJ PJe platform

Potential Targets

Potential victims spanned a broad spectrum of CNJ PJe users, from judges and lawyers to regular citizens, as well as high-profile justice, government, and military officials such as prosecutors and ministers.

Responsible Disclosure

Immediately after the vulnerability was found, an advisory describing details of the issue, attack scenarios, and proof-of-concept was reported to CNJ's PJe technical team at the Pernambuco Court of Justice (TJPE). The issue was fixed shortly thereafter[4].

- IOActive releases an advisory detailing the issue - March 2, 2021[5].

Man-in-the-Middle (MITM) Attack

Man-in-the-middle attacks are a widespread risk in shared working environments (such as those often used while traveling). What is less well-known is how easy it is for relatively unsophisticated attackers to leverage these kinds of attacks against people working from home; one of the most common attack types of this kind that we see are DNS spoofing and cache poisoning attacks against home WiFi/broadband routers[6] commonly distributed by residential internet providers.

Whether our target is traveling or working from home, an attacker has a multitude of options that he can utilize to carry out a MITM attack against a specific target:

- Use of open WiFi; for example, in restaurants, hotels, conference centers, airports, shared office working spaces, and overall public Internet access
- ARP spoofing attacks against shared networks
- Compromise of an ISP, home router, WiFi repeater, or other network infrastructure component
- DNS spoofing or cache poisoning attacks

Attack Illustration

Every time PJeOffice is launched, it asks CNJ's system if a newer version of the application is available. When available, the user is offered an update for installation on their computer. [figure 1]

Due to the lack of secure communications, an attacker—positioning himself as a man-In-the-middle—can intercept the traffic between the user and CNJ's infrastructure, finally redirecting the legitimate update request to a server under his control. [figure 2]

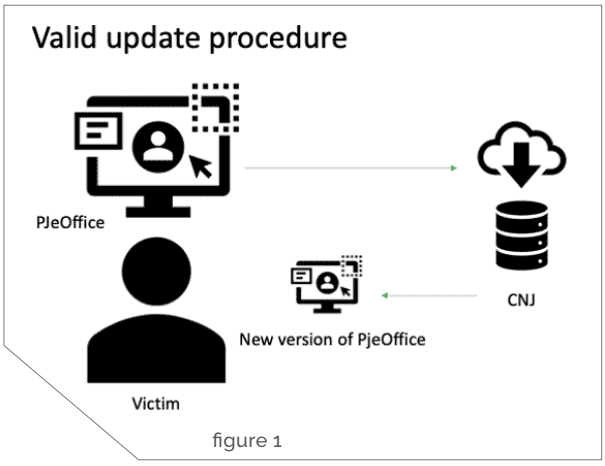

figure 1

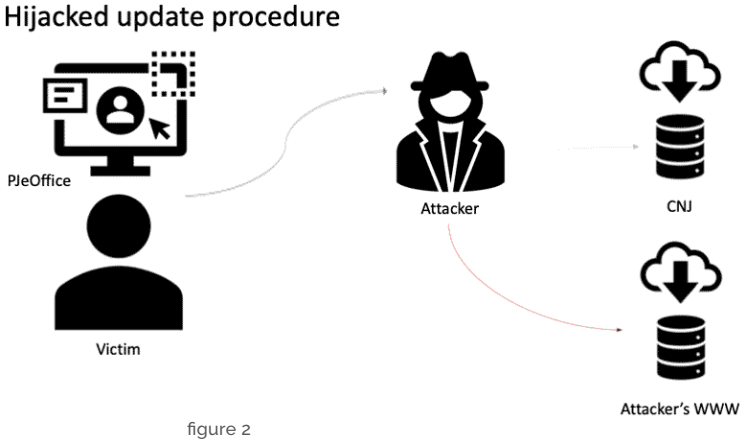

figure 2

CNJ PJe's platform does not properly validate the integrity and authenticity of the update prior to installation. As such, the attacker is able to force the installation of a forged application on the device of the vulnerable user. [figure 3]

Once the forged PJeOffice update is installed and executed, an attacker can take control over PJeOffice's user account, including all of the user's privileges within the CNJ PJe platform. [figure 4]

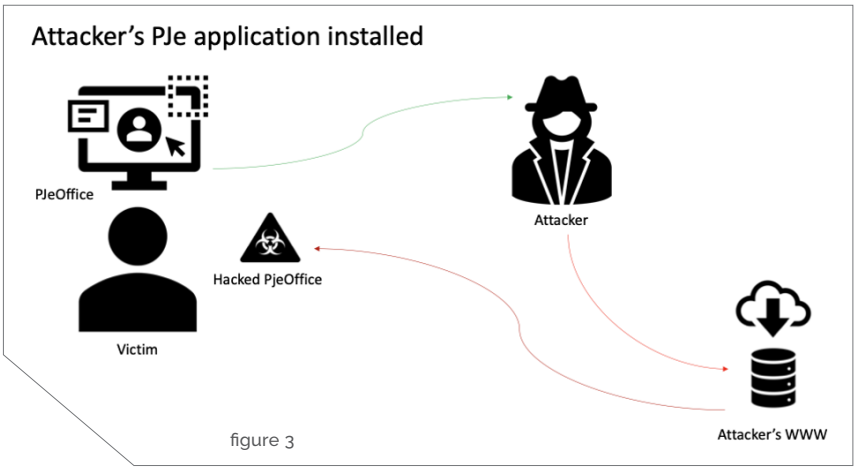

figure 3

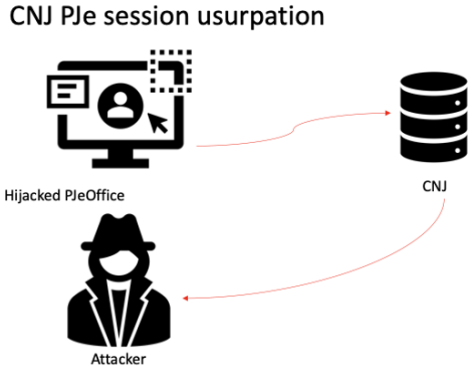

figure 4

If that wasn't bad enough, upon launch of the attacker's specially crafted PJe version, the attacker could take control over the victim's computer, enabling access to documents and data stored on that computer, as well as control over other installed applications. [figure 5]

figure 5

Broader Scope Impact

Well-coordinated attacks could have led to a wide range of compromises, including data breaches and unauthorized access to confidential processual data. Furthermore, a structured attack could use the victim's digital certificates to alter and sign legal procedures within all jurisdictions under CNJ PJe's domain.

Potential fall-out from such attacks could include:

- Government and industrial espionage affecting law firms, corporations and sovereign states alike
- Market manipulation affecting both government institutions and the private sector
- Overall disruption of the judicial system with multiple effects, including the breakage of the "Democracy and Trust" dichotomy

Programs within the public sector are often created to stimulate information security measures and processes, such as adding security to the Software Development Lifecycle (SDLC), but trivial vulnerabilities still threaten governmental infrastructures today, raising the specter of future attacks as easily mounted as the man-in-the-middle attack on CNJ PJe users—with potentially significant consequences.

While Information Security has strongly evolved over the past several decades, creating solid engineering, processual, and cultural solutions. New directions in the way we depend upon and use technology will come with issues that are not necessarily new or complex.

1 http://www.brazil.gov.br/government/how-the-government-works/federal-judiciary-branch
2 https://www.cnj.jus.br/wiki/index.php/PJeOffice
3 https://en.wikipedia.org/wiki/Jurimetrics
4 https://www.cnj.jus.br/nova-versao-do-pjeoffice-torna-atualizacao-automatica/
5 https://ioactive.com/cnj-pjeoffice-remote-code-execution-in-update-mechanism/
6 https://cujo.com/dns-hijacking-attacks-on-home-routers-in-brazil/