**广西移动信息门户**

**渗透测试报告**

**DeepTide\_Lab(深汐安全实验室)**

**2017年5月22日**

**文档控制**

|  |  |
| --- | --- |
| 拟 制: |  |
| 审 核: |  |
| 标准化: |  |
| 读 者： | 上海移动相关成员 |

**保密申明**

这份文档涉及到DeepTide\_Lab商业秘密信息。接受这份说明书表示同意对其内容保密，未经书面请求并得到DeepTide\_Lab的书面认可，不得复制，泄露或散布这份文档。如果你不是有意接受者，请注意对这份文档内容的任何形式的泄露、复制或散布都有可能引起法律纠纷。

目录

[第一章. 渗透测试结果 5](#_Toc483246751)

[2.1 [高危] 敏感信息明文传输 5](#_Toc483246754)

[2.2 [中危] 无验证码机制 6](#_Toc483246755)

[2.3 [高危] 账户弱口令 7](#_Toc483246756)

[2.4 [高危] dubbo admin弱口令 9](#_Toc483246757)

[2.5 [高危] Tomcat弱口令 10](#_Toc483246758)

[2.6 [高危] Active MQ弱口令 10](#_Toc483246759)

[2.7 [高危] S2-009、S2-016命令执行 11](#_Toc483246760)

[2.8 [高危] S2-045、S2-046命令执行 12](#_Toc483246761)

[2.9 [高危] SQL注入 15](#_Toc483246762)

[2.10 [高危] 越权之敏感信息泄露 20](#_Toc483246763)

[2.11 [中危] URL重定向 21](#_Toc483246764)

[2.12 [高危] 心脏出血漏洞（Heartbleed bug） 22](#_Toc483246765)

[2.13 [高危] Redis未授权访问 23](#_Toc483246766)

[2.14 [高危] ElasticSearch未授权访问 24](#_Toc483246767)

[2.15 [高危] Weblogic JAVA反序列化 远程命令执行 25](#_Toc483246768)

[2.16 [中危] Memcache未授权访问 26](#_Toc483246769)

[2.17 [高危] ORACLE TNS Listener远程投毒 27](#_Toc483246770)

[2.18 [中危] Apache Tomcat样例目录导致session操纵、信息泄露等多个漏洞 28](#_Toc483246771)

[2.19 [高危] Weblogic SSRF漏洞 29](#_Toc483246772)

[2.20 [中危] 默认密码自动填充 31](#_Toc483246773)

[2.21 [高危] 越权访问 32](#_Toc483246774)

[2.22 [高危] 设计缺陷之任意账户登陆 32](#_Toc483246775)

[2.23 [高危] 任意文件读取漏洞 33](#_Toc483246776)

[2.24 [中危] 目录列表 34](#_Toc483246777)

[2.25 [中危] 验证码绕过 36](#_Toc483246778)

[2.26 [高危] Weblogic JAVA反序列化 远程命令执行 36](#_Toc483246779)

[2.27 [中危] 密码字段明文显示 37](#_Toc483246780)

[2.28 [中危] Apache Jserv协议服务对外开放 38](#_Toc483246781)

[2.29 [高危] Redis未授权访问 39](#_Toc483246782)

[2.30 [高危] HP Application Management Business Process Monitor 管理后台未授权访问 40](#_Toc483246783)

[2.31 [高危] Active MQ未授权访问 41](#_Toc483246784)

[2.32 [高危] BES管理控制台弱口令 42](#_Toc483246785)

[2.33 [高危] XSS漏洞 43](#_Toc483246786)

[2.34 [中危] CRLF注入 48](#_Toc483246787)

[2.35 [中危] HOST头攻击 50](#_Toc483246788)

[2.36 [高危] SVN信息泄露 51](#_Toc483246789)

1. 渗透测试结果
3. 1. [高危] 敏感信息明文传输++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 敏感信息明文传输 | **风险级别** | 高 |
| **风险描述** | 敏感信息明文传输，一旦遭遇中间人攻击则攻击者将能够轻而易举获得敏感信息，其中包括用户名和密码敏感信息明文传输等敏感信息。 | | |
| **漏洞URL** | <http://10.182.20.44/shared/userlogin.php>  <http://10.182.20.45/shared/userlogin.php>  <http://10.182.20.46/shared/userlogin.php>  <http://10.182.20.42:19003/npage/login/login.htm>  <http://10.182.20.48:28077/>  update  [172.20.35.44:8088](http://172.20.35.44:8088)  [10.182.20.43:8885](http://10.182.20.43:8885)  10.182.13.179:6001  10.182.13.241:9001  10.182.13.241:9002  10.182.13.241:9003  10.182.13.241:9005  10.182.13.241:9006  10.182.13.241:9007  10.182.13.242:9001  10.182.13.242:9002  10.182.13.242:9006  10.182.13.242:9007  10.182.13.243:9001  10.182.13.243:9003  10.182.13.243:9005  10.182.13.243:9006  10.182.13.243:9007  10.182.20.42:19003  172.20.35.71:9001  172.20.35.71:9002  172.20.35.71:9003 | | |
| **漏洞验证** |  | | |
| **整改建议** | 敏感信息加密传输 | | |

* 1. [中危] 无验证码机制++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 无验证码机制 | **风险级别** | 中 |
| **风险描述** | 无验证码机制，这导致攻击者能够进行暴力破解。 | | |
| 漏洞URL | <http://10.182.20.42:19003/npage/login/login.htm>  <http://10.182.20.42:39080>  <http://10.182.20.48:28077/>  <http://10.182.20.43:8885>  update  <http://172.20.35.44:8088>  10.182.13.179:6001  10.182.13.241:9001  10.182.13.241:9002  10.182.13.241:9003  10.182.13.241:9005  10.182.13.241:9006  10.182.13.241:9007  10.182.13.242:9001  10.182.13.242:9002  10.182.13.242:9006  10.182.13.242:9007  10.182.13.243:9001  10.182.13.243:9003  10.182.13.243:9005  10.182.13.243:9006  10.182.13.243:9007  10.182.20.42:19003  172.20.35.71:9001  172.20.35.71:9002  172.20.35.71:9003 | | |
| **漏洞验证** |  | | |
| **整改建议** | 添加验证码机制,多次登录失败后锁定账户一段时间 | | |

* 1. [高危] 账户弱口令++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 账户弱口令 | **风险级别** | 高 |
| **风险描述** | 发现存在弱口令，这将直接导致恶意攻击者掌握账户信息，并可能导致伪造合法用户进行非法操作。 | | |
| **漏洞URL** | <http://10.182.38.40:8001>  admin/admin  <http://10.182.20.43:8885>  admin/admin  <http://10.182.20.48:28077>  update  <http://172.20.35.44:8088> | | |
| **漏洞验证** | admin/admin    admin/admin    admin/12345678    admin/admin | | |
| **整改建议** | 杜绝弱口令，修改得越复杂越好，并且定期更换密码，最好修改密码策略，强制要求用户输入强密码，加强员工安全意识。 | | |

* 1. [高危] dubbo admin弱口令

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | dubbo admin弱口令 | **风险级别** | 高 |
| **风险描述** | dubbo可以集中管理各个服务提供者、消费者集群，并提供注册中心、性能监控和管理后台等功能，dubbo admin存在弱口令，攻击者可直接登录dubbo admin后台，严重威胁。 | | |
| **漏洞URL** | <http://10.182.38.203:30881/>  root/root | | |
| **漏洞验证** |  | | |
| **整改建议** | 更改弱口令 | | |

* 1. [高危] Tomcat弱口令

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Tomcat弱口令 | **风险级别** | 高 |
| **风险描述** | 攻击者可以利用此漏洞在受影响的服务器上安装恶意应用程序，并使用Tomcat的权限运行任意代码。 | | |
| **漏洞URL** | http://10.182.20.42:18061  admin/admin  <http://10.182.20.42:11110/manager/html>  tomcat/tomcat  <http://172.20.35.29:20500>  admin/admin | | |
| **漏洞验证** |  | | |
| **整改建议** | 更改弱口令 | | |

* 1. [高危] Active MQ弱口令

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Tomcat弱口令 | **风险级别** | 高 |
| **风险描述** | 攻击者可以利用登陆后台，可能导致攻击者后续高级攻击，包括getshell等。 | | |
| **漏洞URL** | <http://10.182.20.38:16166/admin>  admin/admin  user/user | | |
| **漏洞验证** |  | | |
| **整改建议** | 更改弱口令 | | |

* 1. [高危] S2-009、S2-016命令执行

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | S2-016命令执行 | **风险级别** | 高 |
| **风险描述** | 攻击者可以通过操纵参数远程执行恶意代码。Struts 2.3.15.1之前的版本，参数action的值redirect以及redirectAction没有正确过滤，导致ognl代码执行。 | | |
| **漏洞URL** | **示例：**  **http://10.182.38.202:51010/special/stoVisual/showStoPreview.action** | | |
| **漏洞验证** |  | | |
| **整改建议** | 更新补丁到最新版本 | | |

* 1. [高危] S2-045、S2-046命令执行

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | S2-045命令执行 | **风险级别** | 高 |
| **风险描述** | Apache Struts 2被曝存在远程命令执行漏洞，漏洞编号S2-045，CVE编号CVE-2017-5638，在使用基于Jakarta插件的文件上传功能时，有可能存在远程命令执行，导致系统被黑客入侵。 | | |
| **漏洞URL** | [**http://10.182.38.202:8666/portal//ibnms/report/addModuleUseLog.action**](http://10.182.38.202:8666/portal//ibnms/report/addModuleUseLog.action)  [**http://10.185.15.202:8094/smp/smp/workPlan!getWorkPlanList.action**](http://10.185.15.202:8094/smp/smp/workPlan!getWorkPlanList.action) | | |
| **漏洞验证** |  | | |
| **整改建议** | 升级core的jar包、核心包升级下  需要替换的jar包: struts2-core-2.3.32.jar、xwork-core-2.3.32.jar、struts2-json-plugin-2.3.32.jar  需要添加的jar包: commons-lang3-3.2.jar、javassist-3.11.0.GA.jar  保留的jar包: commons-lang-2.4.jar  可能需要添加的jar包: commons-fileupload-1.3.2.jar、freemarker-2.3.22.jar、ognl-3.0.19.jar 、ognl-3.0.19.jar  、commons-logging-1.1.3.jar  官方补丁下载地址:  https://dist.apache.org/repos/dist/release/struts/2.3.32/ https://dist.apache.org/repos/dist/release/struts/2.5.10.1/ | | |

* 1. [高危] SQL注入

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | SQL注入 | **风险级别** | 高 |
| **风险描述** | 导致攻击者不仅可以获取网站数据，还可以直接生成网站后门，后门程序可以得到web用户的所有权限，包括对数据库的增删改查，文件的修改等。 | | |
| **漏洞URL** | 所有涉及到查询的接口都存在类似问题，这里以部分功能点进行验证：  标红的都是存在问题的：  POST /itil/getHostAccountsInfoList.do?getJson=true HTTP/1.1  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Accept: application/json, text/javascript, \*/\*; q=0.01  X-Requested-With: XMLHttpRequest  Referer: http://10.182.38.202:8666/itil/getHostAccountsInfoList.do?0.4b8ydan6tdvp#  Accept-Language: zh-cn  Accept-Encoding: gzip, deflate  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko  Host: 10.182.38.202:8666  Content-Length: 120  Pragma: no-cache  Cookie: JSESSIONID=9A83F28B3A3A8574D4F9439EC5C5889D; JSESSIONID=862EA419EBA0991164ADD4E09D4F9BD7  Connection: close  host\_ip=10.182.13.129&host\_name=ng3-cbossdb1&host\_user=backadm&remaining\_time=100&user\_type=3&pri\_person=&page=1&rows=50  POST /itil/findPersonalTasks.do?pagesize=15&processId=&wf\_num=ZC2017050980244&func\_title=%25E5%2585%25B3%25E4%25BA%258E%25E7%2594%25B3%25E8%25AF%25B7%25E8%25BF%259B%25E8%25A1%258C%25E6%2598%2586%25E8%2585%25BE%25E7%25A3%2581%25E5%25B8%25A6%25E5%25BA%2593%25E5%25AE%2589%25E5%2585%25A8%25E6%2589%25AB%25E6%258F%258F%25E7%259A%2584%25E7%2594%25B3%25E8%25AF%25B7&employee=&time=Thu%20May%2018%2016:40:14%20UTC+0800%202017&processGroupId=1&confirm\_type=&orderByValue= HTTP/1.1  Content-Type: application/x-www-form-urlencoded  X-Requested-With: XMLHttpRequest  Accept: application/json, text/javascript, \*/\*  Referer: http://10.182.38.202:8666/itil/itsm/MyWorkBench.jsp  Accept-Language: zh-cn  Accept-Encoding: gzip, deflate  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko  Host: 10.182.38.202:8666  Content-Length: 47  Pragma: no-cache  Cookie: JSESSIONID=9A83F28B3A3A8574D4F9439EC5C5889D; JSESSIONID=862EA419EBA0991164ADD4E09D4F9BD7  Connection: close  PAGINATION\_CURRENT\_PAGE\_NO=1&sortType=5&sqlStr=  POST /itil/loadSupportWorkorderList.do HTTP/1.1  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Accept: application/json, text/javascript, \*/\*; q=0.01  X-Requested-With: XMLHttpRequest  Referer: http://10.182.38.202:8666/itil/showSupportWorkorderPage.do#  Accept-Language: zh-cn  Accept-Encoding: gzip, deflate  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; Touch; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Tablet PC 2.0)  Host: 10.182.38.202:8666  Content-Length: 202  Pragma: no-cache  Cookie: JSESSIONID=9A83F28B3A3A8574D4F9439EC5C5889D; JSESSIONID=862EA419EBA0991164ADD4E09D4F9BD7  Connection: close  startTime=2017-04-18&endTime=2017-05-18&queryType=&taskLevel=&status=&wfNum=ZC2017051887659&flowType=&levelType=&submitDeptId=&operateDeptId=&content=&currDealerId=&dealerId=&createrId=&getRecordCount=1  POST /AttendanceManageListUILoad.do HTTP/1.1  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Accept: application/json, text/javascript, \*/\*; q=0.01  X-Requested-With: XMLHttpRequest  Referer: http://10.182.38.202:8666/AttendanceManageListUI.do?0.zzmscvkb6e6t#  Accept-Language: zh-cn  Accept-Encoding: gzip, deflate  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko  Host: 10.182.38.202:8666  Content-Length: 130  Pragma: no-cache  Cookie: JSESSIONID=2C4494F74655CF56BE3099634D8F8629  Connection: close  DUTY\_DEPT\_ID=100&DUTY\_LOGIN\_ID=hetiantian1&apply\_type=1022337&time\_start=2017-02-01&time\_end=2017-05-19&type=search&page=1&rows=20  POST /loadListMessageGroupManageDatas.do?message\_team\_id=&groupedit= HTTP/1.1  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Accept: application/json, text/javascript, \*/\*; q=0.01  X-Requested-With: XMLHttpRequest  Referer: http://10.182.38.202:8666/loadListMessageGroupManage.do?ticket=ST-3019-2CICVUU6TeZBWYqZ69If-cas  Accept-Language: zh-cn  Accept-Encoding: gzip, deflate  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko  Host: 10.182.38.202:8666/loadListMessageGroupManageDatas.do?message\_team\_id=&groupedit=  Content-Length: 294  Pragma: no-cache  Cookie: JSESSIONID=2C4494F74655CF56BE3099634D8F8629  Connection: close  flag=search&S\_DEPT=%2520%25E6%25B2%25B3%25E6%25B1%25A0%25E5%25AE%25A2%25E6%2588%25B7%25E5%2593%258D%25E5%25BA%2594%25E4%25B8%25AD%25E5%25BF%2583%2520&S\_NAME=%25E9%25BB%2584%25E5%25AE%2587&S\_PHONE=018807780123&type\_id=1&beginDate=undefined&endDate=undefined&S\_ENABLE=&searchFlag=1&page=1&rows=15 | | |
| **漏洞验证** |  | | |
| **整改建议** | 推荐参数化查询或参数过滤，并排查其它类似参数 | | |

* 1. [高危] 越权之敏感信息泄露

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 越权之敏感信息泄露 | **风险级别** | 高 |
| **风险描述** | 设计不合理、导致恶意攻击者能够轻易获取众多敏感信息。 | | |
| **漏洞URL** | POST /itil/loadAttendanceRecord.do?getJson=true&fromPage=all HTTP/1.1  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  Accept: application/json, text/javascript, \*/\*; q=0.01  X-Requested-With: XMLHttpRequest  Referer: http://10.182.38.202:8666/itil/openPsKqViewPage.do?0.8n3vchcn8y7o#  Accept-Language: zh-cn  Accept-Encoding: gzip, deflate  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko  Host: 10.182.38.202:8666  Content-Length: 68  Pragma: no-cache  Cookie: JSESSIONID=9A83F28B3A3A8574D4F9439EC5C5889D; JSESSIONID=862EA419EBA0991164ADD4E09D4F9BD7  Connection: close  starttime=2017-02-18&endtime=&att\_status=&aud\_status=&page=1&rows=20 | | |
| **漏洞验证** |  | | |
| **整改建议** | 更改设计，控制权限 | | |

* 1. [中危] URL重定向

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | URL重定向 | **风险级别** | 中 |
| **风险描述** | 服务端未对传入的跳转url变量进行检查和控制，可能导致可恶意构造任意一个恶意地址，诱导用户跳转到恶意网站。由于是从可信的站点跳转出去的，用户会比较信任，所以跳转漏洞一般用于钓鱼攻击，通过转到恶意网站欺骗用户输入用户名和密码盗取用户信息，或欺骗用户进行金钱交易。 | | |
| **漏洞URL** | http://10.182.38.202:8666/cas/login?service=http%3a%2f%2fwww.baidu.com%2fa%3fhttp%3a%2f%2f10.182.38.202%3a8666%2fhostAll.do%3fmodule\_id%3dm010601100%26kbp\_id%3d10-10&systemId=1012 | | |
| **漏洞验证** |  | | |
| **整改建议** | 禁止跳转或者跳转的时候对url进行校验。 | | |

* 1. [高危] 心脏出血漏洞（Heartbleed bug）

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 心脏出血漏洞（Heartbleed bug） | **风险级别** | 高 |
| **风险描述** | 经由心脏出血漏洞发动攻击，获得的数据可能包括TLS双方将要交换、但尚未加密的机密内容，包括在用户请求中各种格式的post数据。此外，泄漏的数据还可能含有身份验证密令，如会话cookie及密码，可使攻击者向该服务冒充此用户。  攻击还可能泄漏受攻击双方的私钥，这将使攻击者能解密通信内容（将来或是之前通过被动窃听捕获而存储的通信，除非使用完全正向保密，而在这种情况下，只能解密将来通过中间人攻击截获的通信）。 | | |
| **漏洞地址** | 10.182.38.103 :443  10.182.38.101 :443 | | |
| **漏洞验证** |  | | |
| **整改建议** | 更新OpenSSL | | |

* 1. [高危] Redis未授权访问++100

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Redis未授权访问 | **风险级别** | 高 |
| **风险描述** | 存在Redis未授权访问，没有开启认证的情况下，可以导致任意用户在可以访问目标服务器的情况下未授权访问 Redis 以及读取 Redis 的数据。攻击者在未授权访问 Redis 的情况下可以利用 Redis 的相关方法，可以成功在 Redis 服务器上写入公钥，进而可以使用对应私钥直接登录目标服务器 | | |
| **漏洞ip** | 10.182.20.42:37895  update:  10.182.20.42:37891  10.182.20.42:37892  10.182.20.42:37893  10.182.20.42:37894  10.182.20.42:56379  10.182.39.28:6637  10.182.39.29:6637  10.182.39.30:6637  10.182.39.31:6637  10.182.39.32:6637  10.182.39.33:6637  172.20.32.20:6379  172.20.35.23:6379  172.20.35.29:56379  172.20.35.29:6379  172.20.35.30:20002  172.20.35.30:20003  172.20.35.30:25001  172.20.35.30:25002  172.20.35.30:56379  172.20.35.30:6379  172.20.35.30:7379  172.20.35.31:20001  172.20.35.31:20002  172.20.35.31:20003  172.20.35.31:56379  172.20.35.31:6379  172.20.35.31:7379  172.20.35.31:9379  172.20.35.37:6379  172.20.35.37:7000  172.20.35.37:7010  172.20.35.37:7020  172.20.35.37:7030  172.20.35.37:7040  172.20.35.37:7050  172.20.35.38:20011  172.20.35.38:20012  172.20.35.38:20021  172.20.35.38:20022  172.20.35.38:20031  172.20.35.38:20032  172.20.35.40:20011  172.20.35.40:20012  172.20.35.40:20021  172.20.35.40:20022  172.20.35.40:20031  172.20.35.40:20032  172.20.35.41:20011  172.20.35.41:20012  172.20.35.44:20011  172.20.35.46:20021  172.20.35.47:20021  172.20.35.47:20022  172.20.35.47:20031  172.20.35.47:20032  172.20.35.47:38001  172.20.35.47:38002  172.20.35.47:38003  172.20.35.47:38004  172.20.35.48:20021  172.20.35.48:20022  172.20.35.48:20031  172.20.35.48:20032  172.20.35.48:6379 | | |
| **漏洞验证** |  | | |
| **整改建议** | 1. redis.conf: bind 127.0.0.1  //redis本来就是作为内存数据库，只要监听在本机即可  2. 配置认证，也就是AUTH，设置密码，密码会以明文方式保存在Redis配置文件中  3. 限定可以连接Redis服务器的IP  4. 修改Redis默认端口6379  5. 配置rename-command配置项"RENAME\_CONFIG"，这样即使存在未授权访问，也能够给攻击者使用config 指令加大难度  6. 禁止使用 root 权限启动 redis 服务 | | |

* 1. [高危] ElasticSearch未授权访问++14

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | ElasticSearch未授权访问 | **风险级别** | 高 |
| **风险描述** | 存在ElasticSearch未授权访问漏洞。ElasticSearch是一个基于Lucene的搜索服务器。它提供了一个分布式多用户能力的全文搜索引擎，基于RESTful web接口。Elasticsearch是用Java开发的，并作为Apache许可条款下的开放源码发布，是当前流行的企业级搜索引擎。Elasticsearch未授权访问可导致ES中存储的数据被任意查看。可能导致攻击者利用该漏洞可导致网页被篡改、数据被篡改、核心数据被窃取、数据库所在服务器被攻击变成傀儡主机。 | | |
| **漏洞ip** | 10.182.20.42:3757  10.182.20.42:3778  update：  172.20.35.28:9200  172.20.35.47:9200  172.20.35.38:9201  172.20.35.39:9200  172.20.35.48:9200  172.20.35.38:9200  172.20.35.31:9201  172.20.35.41:9200  172.20.35.29:9200  172.20.35.40:9200  172.20.35.44:9200  172.20.35.46:9200  172.20.35.30:9200  172.20.35.40:9201 | | |
| **漏洞验证** |  | | |
| **整改建议** | 在config/elasticsearch.yml中为相应端口设置认证：  http.basic.enabled true #开关，开启会接管全部HTTP连接  http.basic.user "admin" #账号  http.basic.password "admin\_pw" #密码  http.basic.ipwhitelist ["localhost", "127.0.0.1"] #白名单内的ip访问不需要通过账号和密码，支持ip和主机名，不支持ip区间或正则  http.basic.trusted\_proxy\_chains [] #信任代理列表  http.basic.log false #把无授权的访问事件添加到ES的日志  http.basic.xforward "" #记载代理路径的header字段名 | | |

* 1. [中危] Memcache未授权访问++22

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Memcache未授权访问 | **风险级别** | 中 |
| **风险描述** | Memcache存在未授权访问，可能导致除memcached中数据可被直接读取泄漏和恶意修改外，由于memcached中的数据像正常网站用户访问提交变量一样会被后端代码处理，当处理代码存在缺陷时会再次导致不同类型的安全问题。 | | |
| **漏洞ip** | 10.182.20.43:11222  10.182.20.42:3784  10.182.20.43:11212  10.182.20.42:36666  update  172.20.35.44:37777  172.20.35.47:36666  172.20.35.40:36666  172.20.35.33:36666  172.20.35.44:31111  172.20.35.41:36666  10.182.20.43:11211  172.20.35.32:36666  172.20.35.25:11212  172.20.35.40:31111  172.20.35.38:31111  172.20.35.46:31111  172.20.35.47:31111  172.20.35.30:31111  172.20.35.25:11211  172.20.35.31:31111  172.20.35.39:31111  172.20.35.28:36666  172.20.35.44:36666  172.20.35.35:36666  172.20.35.34:36666  172.20.35.25:11222 | | |
| **漏洞验证** |  | | |
| **整改建议** | 1、配置memcached监听本地回环地址127.0.0.1。  [root@local ~]# vim /etc/sysconfig/memcached  OPTIONS="-l 127.0.0.1" #设置本地为监听  [root@local ~]# /etc/init.d/memcached restart #重启服务  [root@local ~]# vim /etc/sysconfig/memcached  OPTIONS="-l 127.0.0.1" #设置本地为监听  [root@local ~]# /etc/init.d/memcached restart #重启服务  2、当memcached配置为监听内网IP或公网IP时，使用主机防火墙（iptalbes、firewalld等）和网络防火墙对memcached服务端口进行过滤 | | |

* 1. [高危] ORACLE TNS Listener远程投毒++135

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | ORACLE TNS Listener远程投毒 | **风险级别** | 高 |
| **风险描述** | 攻击者在不提供用户名/密码的情况下，向远程“TNS Listener”组件处理的数据投毒的漏洞。 | | |
| **漏洞地址** | update   |  | | --- | | 10.182.38.50:55464 | | 10.182.38.49:55464 | | 10.182.38.48:39689 | | 10.182.38.48:21846 | | 10.182.38.47:39689 | | 10.182.38.47:21846 | | 10.182.38.46:39689 | | 10.182.38.46:21846 | | 10.182.38.39:47632 | | 10.182.38.39:2521 | | 10.182.38.38:47632 | | 10.182.38.37:47632 | | 10.182.38.36:47632 | | 10.182.38.35:47632 | | 10.182.38.148:3002 | | 10.182.38.146:3002 | | 10.182.39.34:1521 | | 10.182.39.160:3003 | | 10.182.39.158:3003 | | 10.182.38.50:55464 | | 10.182.38.49:55464 | | 10.182.38.48:39689 | | 10.182.38.48:21846 | | 10.182.38.47:39689 | | 10.182.38.47:21846 | | 10.182.38.46:39689 | | 10.182.38.46:21846 | | 10.182.38.39:47632 | | 10.182.38.39:2521 | | 10.182.38.38:47632 | | 10.182.38.37:47632 | | 10.182.38.36:47632 | | 10.182.38.35:47632 | | 10.182.38.148:3002 | | 10.182.38.146:3002 | | 172.20.35.79:2700 | | 172.20.35.78:2700 | | 172.20.35.75:2700 | | 172.20.35.75:1521 | | 172.20.35.72:2700 | | 172.20.35.71:2700 | | 172.20.35.62:2800 | | 172.20.35.62:2700 | | 172.20.35.61:2800 | | 172.20.35.61:2700 | | 172.20.35.60:2800 | | 172.20.35.60:2700 | | 172.20.35.59:2800 | | 172.20.35.59:2700 | | 172.20.35.58:2800 | | 172.20.35.58:2700 | | 10.182.32.200:2521 | | 10.182.20.48:2700 | | 10.182.20.46:3000 | | 10.182.20.46:2700 | | 10.182.20.45:2700 | | 10.182.20.42:60045 | | 10.182.20.42:60019 | | 10.182.20.42:13000 | | 10.182.20.42:9130 | | 10.182.20.42:9201 | | 10.182.20.42:9203 | | 10.182.20.42:9204 | | 10.182.20.42:9210 | | 10.182.20.42:9303 | | 10.182.20.42:9401 | | 10.182.20.42:9402 | | 10.182.20.42:9403 | | 10.182.20.42:9404 | | 10.182.20.42:9405 | | 10.182.20.42:9661 | | 10.182.20.42:9662 | | 10.182.20.42:10085 | | 10.182.20.42:11521 | | 10.182.20.42:11525 | | 10.182.20.42:13000 | | 10.182.20.42:60019 | | 10.182.20.42:60045 | | 10.182.20.45:2700 | | 10.182.20.46:2700 | | 10.182.20.46:3000 | | 10.182.20.48:2700 | | 10.182.32.200:2521 | | 172.20.35.58:2700 | | 172.20.35.58:2800 | | 172.20.35.59:2700 | | 172.20.35.59:2800 | | 172.20.35.60:2700 | | 172.20.35.60:2800 | | 172.20.35.61:2700 | | 172.20.35.61:2800 | | 172.20.35.62:2700 | | 172.20.35.62:2800 | | 172.20.35.71:2700 | | 172.20.35.72:2700 | | 172.20.35.75:1521 | | 172.20.35.75:2700 | | 172.20.35.78:2700 | | 172.20.35.79:2700 | | 10.182.38.146:3002 | | 10.182.38.148:3002 | | 10.182.38.35:47632 | | 10.182.38.36:47632 | | 10.182.38.37:47632 | | 10.182.38.38:47632 | | 10.182.38.39:2521 | | 10.182.38.39:47632 | | 10.182.38.46:21846 | | 10.182.38.46:39689 | | 10.182.38.47:21846 | | 10.182.38.47:39689 | | 10.182.38.48:21846 | | 10.182.38.48:39689 | | 10.182.38.49:55464 | | 10.182.38.50:55464 | | 10.182.39.158:3003 | | 10.182.39.160:3003 | | 10.182.39.34:1521 | | 10.182.38.146:3002 | | 10.182.38.148:3002 | | 10.182.38.35:47632 | | 10.182.38.36:47632 | | 10.182.38.37:47632 | | 10.182.38.38:47632 | | 10.182.38.39:2521 | | 10.182.38.39:47632 | | 10.182.38.46:21846 | | 10.182.38.46:39689 | | 10.182.38.47:21846 | | 10.182.38.47:39689 | | 10.182.38.48:21846 | | 10.182.38.48:39689 | | 10.182.38.49:55464 | | 10.182.38.50:55464 | | | |
| **漏洞验证** |  | | |
| **整改建议** | 参考官方建议, <http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html> | | |

* 1. [中危] Apache Tomcat样例目录导致session操纵、信息泄露等多个漏洞++22

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Apache Tomcat样例目录session操纵漏洞、信息泄露等多个漏洞 | **风险级别** | 中 |
| **风险描述** | 攻击者可通过此漏洞操作cookie以及Session等。 | | |
| **漏洞URL** | http://10.182.15.85:18888/examples  http://10.182.15.85:28888/examples  http://10.182.20.32:8080/examples  http://10.182.20.33:12315/examples  http://10.182.20.42:13333/examples  http://10.182.20.42:21112/examples  http://10.182.20.42:39081/examples  http://10.182.20.42:3929/examples  http://10.182.20.42:3930/examples  http://10.182.20.42:3951/examples  http://10.182.20.42:4000/examples  http://10.182.20.42:5050/examples  http://10.182.20.42:60057/examples  http://10.182.20.42:60058/examples  http://10.182.20.42:60064/examples  http://10.182.20.42:60065/examples  http://10.182.20.42:9511/examples  http://10.182.20.42:9901/examples  http://10.182.20.42:9908/examples  http://10.182.20.43:1131/examples  http://10.182.20.43:2131/examples  http://10.182.20.48:9092/examples  http://10.182.32.131:7090/examples  http://10.182.38.201:18888/examples  <http://10.182.38.201:28888/examples>  update  10.182.20.42:13333  172.20.32.22:16080  172.20.35.18:18086  172.20.35.23:18084  172.20.35.29:20500  172.20.35.38:21112  172.20.35.39:21111  172.20.35.39:21112  172.20.35.40:21111  172.20.35.44:21112  172.20.35.44:22222  172.20.35.44:8088  172.20.35.45:21111  172.20.35.45:8080  172.20.35.46:21112  172.20.35.48:18088  172.20.35.48:26111  172.20.35.48:36112  172.20.35.48:8081  172.20.35.48:8082  172.20.35.48:8085  172.20.35.49:6060 | | |
| **漏洞验证** |  | | |
| **整改建议** | 删除examples目录 | | |

* 1. [高危] Weblogic SSRF漏洞++33

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Weblogic SSRF漏洞 | **风险级别** | 高 |
| **风险描述** | weblogic 10.0.2 -- 10.3.6版本的SearchPublicRegistries.jsp处会引起SSRF漏洞,利用该漏洞可能探测内网，攻击内网或本地程序、对内网web应用进行指纹识别、实现多种攻击，读取文件等。 | | |
| **漏洞URL** | http://10.182.13.241:6001  http://10.182.13.242:6001  http://10.182.13.243:6001  http://10.182.20.34:31001  http://10.182.20.34:31002  http://10.182.20.34:31003  http://10.182.20.34:31004  http://10.182.20.34:31005  http://10.182.20.34:31006  http://10.182.20.34:34007  http://10.182.20.34:51001  http://10.182.20.34:51007  http://10.182.20.34:8090  http://10.182.20.34:9001  http://10.182.20.38:11001  http://10.182.20.38:8081  http://10.182.20.38:8094  http://10.182.20.38:9101  http://10.182.20.38:9102  http://10.182.20.38:9103  http://10.182.20.38:9104  http://10.182.20.38:9105  http://10.182.20.38:9201  http://10.182.20.38:9202  http://10.182.20.38:9203  http://10.182.20.39:7002  http://10.182.20.39:9001  http://10.182.20.42:8102  http://10.182.20.42:8103  http://10.182.20.42:8104  http://10.182.20.42:9991  http://10.182.20.42:9996  http://10.182.21.51:7001  http://10.182.22.21:10001  http://10.182.22.22:10001  http://10.182.38.40:16001  http://10.182.38.40:26001  http://10.182.38.40:6001  http://10.185.22.188:6001  http://10.185.22.195:6001  <http://10.185.22.208:6001>  <http://10.182.20.42:19003>  <http://10.182.20.38:8093>  update  172.20.35.71:9001  172.20.35.71:9002  172.20.35.71:9003  10.182.13.13:10001  10.182.13.161:10001  10.182.13.25:10001  10.182.13.25:7201  10.182.20.34:9877  10.182.20.38:8083  10.182.38.40:18001  172.20.35.75:6002  172.20.35.75:9001  172.20.35.79:60001  172.20.35.79:60005  172.20.35.79:6003  172.20.35.79:6013  172.20.35.79:6015  172.20.35.79:6017  172.20.35.79:6019  172.20.35.19:18081  172.20.35.75:8001  172.20.35.19:18082  172.20.35.20:18083  172.20.35.20:18085  172.20.35.75:6001  172.20.35.19:18080  172.20.35.20:18081  172.20.35.19:18084  172.20.35.20:18082  172.20.35.19:18083  172.20.35.20:18080  172.20.35.75:8002  172.20.35.19:7001 | | |
| **漏洞验证** | http://10.182.20.42:9996/uddiexplorer/SearchPublicRegistries.jsp?operator=http://localhost:65535&rdoSearch=name&txtSearchname=sdf&txtSearchkey=&txtSearchfor=&selfor=Business+location&btnSubmit=Search | | |
| **整改建议** | 更新补丁或者禁止访问UDDI | | |

* 1. [中危] 默认密码自动填充

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 默认密码自动填充 | **风险级别** | 中 |
| **风险描述** | 默认密码自动填充，可能为攻击者后续高级攻击做准备。 | | |
| **漏洞URL** | <http://10.182.20.42:39080> | | |
| **漏洞验证** |  | | |
| **整改建议** | 密码不建议自动填充 | | |

* 1. [高危] 越权访问

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 越权访问 | **风险级别** | 高 |
| **风险描述** | 用户未授权的情况下能够越权访问需要授权情况下才能访问的内容，可能导致信息泄露，或者攻击者根据越权页面进行其余漏洞的挖掘。 | | |
| **漏洞URL** | <http://10.182.20.42:39080/acwsui/pages/indexPage/index.htm> | | |
| **漏洞验证** |  | | |
| **整改建议** | 权限控制 | | |

* 1. [高危] 设计缺陷之任意账户登陆

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 设计缺陷之任意账户登陆 | **风险级别** | 高 |
| **风险描述** | 设计不合理、输入任意账户或者密码都能跳转到主页面，可能导致信息泄露、为后续黑客攻击做准备。 | | |
| **漏洞URL** | http://10.182.20.42:39080 | | |
| **漏洞验证** |  | | |
| **整改建议** | 更改设计，登陆校验 | | |

* 1. [高危] 任意文件读取漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 任意文件读取漏洞 | **风险级别** | 高 |
| **风险描述** | 攻击者可以对服务器的任意文件读取，可能导致敏感信息泄露等。 | | |
| **漏洞URL** | 10.182.20.42:60017  10.182.20.42:60048  10.182.20.42:60049  10.182.20.42:60062  10.182.20.42:60063  10.182.20.42:9505  10.182.20.42:9521  10.182.20.42:9524  10.182.20.42:9537  10.182.20.42:9538  10.182.20.42:9793  10.182.20.43:36100  10.182.20.43:36200 | | |
| **漏洞验证** | <http://10.182.20.42:60017/showChart.jsp?filename=.././.././.././.././.././.././.././.././.././.././.././.././.././.././.././.././.././../etc/passwd> | | |
| **整改建议** | 限制…/符号 | | |

* 1. [中危] 目录列表

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 目录列表 | **风险级别** | 中 |
| **风险描述** | 开启了目录列表功能，可能导致泄露敏感信息。 | | |
| **漏洞URL** | http://10.182.20.42:9090  <http://10.182.20.42:9512>  http://10.182.20.42:60017/docs/  http://10.182.20.42:60048/docs/  http://10.182.20.42:60049/docs/  http://10.182.20.42:60062/docs/  http://10.182.20.42:60063/docs/  http://10.182.20.42:9521/docs/  http://10.182.20.42:9524/docs/  http://10.182.20.42:9537/docs/  http://10.182.20.42:9538/docs/  http://10.182.20.42:9793/docs/  http://10.182.20.43:36100/docs/  <http://10.182.20.43:36200/docs/>  <http://10.182.20.48:28080/webdav/>  <http://10.182.20.48:28077/system/>  <http://10.182.20.42:11110/images/>  <http://10.182.20.42:60052/images/>  update  <http://10.182.20.42:3801/images/>  http://10.182.20.42:60028/images/ | | |
| **漏洞验证** |  | | |
| **整改建议** | 1：Apache禁止列目录  修改 httpd.conf配置文件：查找 Options Indexes FollowSymLinks，修改为 Options -Indexes；  2:Apache禁止列目录  在www 目录下的修改.htaccess 配置文件，加入 Options -Indexes。  3:Tomcat 禁止列目录  在Tomcat的conf/web.xml文件里把listings值改为false。 | | |

* 1. [中危] 验证码绕过

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 验证码绕过 | **风险级别** | 中 |
| **风险描述** | 验证码绕过，这导致攻击者能够进行暴力破解。 | | |
| **漏洞URL** | http://10.182.32.131:8090/billcheck/router/login,login | | |
| **漏洞验证** |  | | |
| **整改建议** | 更新验证码机制，对登录失败的及时清空session. | | |

* 1. [高危] Weblogic JAVA反序列化 远程命令执行++26

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Weblogic JAVA反序列化 远程命令执行 | **风险级别** | 高 |
| **风险描述** | 利用该漏洞可以直接执行任意系统命令、核心数据被窃取、数据库所在服务器被攻击变成傀儡主机。 | | |
| **漏洞地址** | 10.182.20.42:18092  10.182.20.42:9991  update：  172.20.35.19:18082  172.20.35.79:60005  172.20.35.79:6015  172.20.35.19:7001  172.20.35.79:6019  10.182.20.34:61001  172.20.35.79:6013  172.20.35.75:9001  172.20.35.20:18083  172.20.35.20:18092  10.182.20.34:8090  172.20.35.79:6017  172.20.35.79:6003  172.20.35.20:18085  172.20.35.20:18080  172.20.35.20:18082  172.20.35.19:18084  172.20.35.75:6002  172.20.35.19:18083  172.20.35.19:18080  172.20.35.79:60001  10.182.20.42:19003  172.20.35.19:18081  10.182.13.15:7001  10.182.20.34:51007  172.20.35.20:18081 | | |
| **漏洞验证** |  | | |
| **整改建议** | 1. 升级Weblogic中间件  2. 升级Commons Collections类到2.2以上版本 <http://commons.apache.org/proper/commons-collections/download_collections.cgi>  3、将应用代码中的java.io.ObjectInputStream替换为SerialKiller <https://github.com/ikkisoft/SerialKiller> | | |

* 1. [中危] 密码字段明文显示

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | 密码字段明文显示 | **风险级别** | 中 |
| **风险描述** | 密码字段明文显示，可能导致敏感信息泄露。 | | |
| **漏洞URL** | http://10.182.20.48:28077/login.do | | |
| **漏洞验证** |  | | |
| **整改建议** | 密码字段类型改为password | | |

* 1. [中危] Apache Jserv协议服务对外开放

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Apache Jserv协议服务对外开放 | **风险级别** | 中 |
| **风险描述** | 此服务配置不当可能造成攻击者访问内部数据 | | |
| **漏洞URL** |  | | |
| **漏洞验证** |  | | |
| **整改建议** | 该服务不建议对外开放 | | |

* 1. [高危] HP Application Management Business Process Monitor 管理后台未授权访问

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | HP Application Management Business Process Monitor 管理后台未授权访问 | **风险级别** | 高 |
| **风险描述** | 攻击者可以直接后台，可能导致敏感信息泄露甚至删除实例等恶意操作等。 | | |
| **漏洞URL** | <http://10.182.15.129:2696>  http://10.182.15.151:2696 | | |
| **漏洞验证** |  | | |
| **整改建议** | 权限控制 | | |

* 1. [高危] Active MQ未授权访问

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Tomcat未授权访问 | **风险级别** | 高 |
| **风险描述** | 攻击者可以直接后台，可能导致信息泄露甚getshell等。 | | |
| **漏洞URL** | http://10.182.15.199:8164/admin/ | | |
| **漏洞验证** |  | | |
| **整改建议** | 权限控制 | | |

* 1. [高危] BES管理控制台弱口令++16

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | BES管理控制台弱口令 | **风险级别** | 高 |
| **风险描述** | 攻击者可以进入管理后台，接管后台所有操作。 | | |
| **漏洞URL** | http://10.182.20.42:3792 | admin | 1qaz2wsx  http://10.182.20.42:3797 | admin | 1qaz2wsx  http://10.182.20.42:9791 | admin | admin  http://10.182.20.42:3798 | admin | 1qaz2wsx  http://10.182.20.42:3799 | admin | 1qaz2wsx  http://10.182.20.42:3945 | admin | 1qaz2wsx  http://10.182.20.42:3946 | admin | 1qaz2wsx  http://10.182.20.42:3947 | admin | 1qaz2wsx  http://10.182.20.42:4100 | admin | 1qaz2wsx  update:  http://172.20.35.28:1900 | admin | admin  http://172.20.35.32:1900 | admin | admin  http://172.20.35.35:1900 | admin | admin  http://172.20.35.37:20800 | admin | 1qaz2wsx  http://172.20.35.37:38120 | admin | 1qaz2wsx  http://172.20.35.37:38140 | admin | 1qaz2wsx  http://172.20.35.37:38160 | admin | 1qaz2wsx  http://172.20.35.37:38180 | admin | 1qaz2wsx  http://172.20.35.37:44210 | admin | 1qaz2wsx  http://172.20.35.37:44220 | admin | 1qaz2wsx  http://172.20.35.37:44230 | admin | 1qaz2wsx  http://172.20.35.37:44240 | admin | 1qaz2wsx  http://172.20.35.40:10100 | admin | 1qaz2wsx  http://172.20.35.40:10300 | admin | 1qaz2wsx  http://172.20.35.40:10400 | admin | 1qaz2wsx  http://172.20.35.40:10500 | admin | 1qaz2wsx | | |
| **漏洞验证** |  | | |
| **整改建议** | 更改弱口令 | | |

* 1. [高危] XSS漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | XSS漏洞 | **风险级别** | 高 |
| **风险描述** | 此漏洞可能导致黑客进行针对性攻击,包括窃取用户Cookie，甚至做诱惑点击导致蠕虫等。 | | |
| **漏洞URL** | <http://10.182.20.42:19003/bp004.go> | method  <http://10.182.20.42:19003/npage/portal/work/portal.jsp> | workNo  http://10.182.20.42:11110  http://10.185.22.195:6001/uddiexplorer/SearchPublicRegistries.jsp  http://10.185.22.188:6001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.21.51:7001/uddiexplorer/SearchPublicRegistries.jsp  http://10.185.22.208:6001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.42:9996/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:9103/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.22.21:10001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:9104/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.38.40:16001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.39:9001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:9101/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.42:19003/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:34007/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:51001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:9102/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:8090/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:9001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.42:9991/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.13.243:6001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:8081/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:8093/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.42:8103/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:31004/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.42:8102/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:9202/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:31002/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:51007/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.38.40:26001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.38.40:6001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.13.241:6001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.39:7002/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:31005/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:31001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:31003/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:9105/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:11001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.22.22:10001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.42:8104/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:8094/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.34:31006/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.13.242:6001/uddiexplorer/SearchPublicRegistries.jsp  http://10.182.20.38:9203/uddiexplorer/SearchPublicRegistries.jsp  <http://10.182.20.38:9201/uddiexplorer/SearchPublicRegistries.jsp>  http://10.185.22.195:6001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.185.22.188:6001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.21.51:7001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.185.22.208:6001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.42:9996/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:9103/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.22.21:10001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:9104/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.38.40:16001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.39:9001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:9101/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.42:19003/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:34007/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:51001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:9102/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:8090/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:9001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.42:9991/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.13.243:6001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:8081/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:8093/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.42:8103/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:31004/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.42:8102/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:9202/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:31002/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:51007/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.38.40:26001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.38.40:6001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.13.241:6001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.39:7002/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:31005/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:31001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:31003/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:9105/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:11001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.22.22:10001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.42:8104/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:8094/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.34:31006/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.13.242:6001/uddiexplorer/SetupUDDIExplorer.jsp  http://10.182.20.38:9203/uddiexplorer/SetupUDDIExplorer.jsp  <http://10.182.20.38:9201/uddiexplorer/SetupUDDIExplorer.jsp>  http://10.185.22.195:6001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.185.22.188:6001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.21.51:7001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.185.22.208:6001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.42:9996/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:9103/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.22.21:10001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:9104/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.38.40:16001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.39:9001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:9101/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.42:19003/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:34007/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:51001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:9102/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:8090/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:9001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.42:9991/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.13.243:6001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:8081/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:8093/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.42:8103/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:31004/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.42:8102/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:9202/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:31002/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:51007/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.38.40:26001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.38.40:6001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.13.241:6001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.39:7002/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:31005/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:31001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:31003/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:9105/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:11001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.22.22:10001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.42:8104/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:8094/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.34:31006/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.13.242:6001/uddiexplorer/SearchPrivateRegistries.jsp  http://10.182.20.38:9203/uddiexplorer/SearchPrivateRegistries.jsp  <http://10.182.20.38:9201/uddiexplorer/SearchPrivateRegistries.jsp>  http://10.185.22.195:6001/uddiexplorer/Login.jsp  http://10.185.22.188:6001/uddiexplorer/Login.jsp  http://10.182.21.51:7001/uddiexplorer/Login.jsp  http://10.185.22.208:6001/uddiexplorer/Login.jsp  http://10.182.20.42:9996/uddiexplorer/Login.jsp  http://10.182.20.38:9103/uddiexplorer/Login.jsp  http://10.182.22.21:10001/uddiexplorer/Login.jsp  http://10.182.20.38:9104/uddiexplorer/Login.jsp  http://10.182.38.40:16001/uddiexplorer/Login.jsp  http://10.182.20.39:9001/uddiexplorer/Login.jsp  http://10.182.20.38:9101/uddiexplorer/Login.jsp  http://10.182.20.42:19003/uddiexplorer/Login.jsp  http://10.182.20.34:34007/uddiexplorer/Login.jsp  http://10.182.20.34:51001/uddiexplorer/Login.jsp  http://10.182.20.38:9102/uddiexplorer/Login.jsp  http://10.182.20.34:8090/uddiexplorer/Login.jsp  http://10.182.20.34:9001/uddiexplorer/Login.jsp  http://10.182.20.42:9991/uddiexplorer/Login.jsp  http://10.182.13.243:6001/uddiexplorer/Login.jsp  http://10.182.20.38:8081/uddiexplorer/Login.jsp  http://10.182.20.38:8093/uddiexplorer/Login.jsp  http://10.182.20.42:8103/uddiexplorer/Login.jsp  http://10.182.20.34:31004/uddiexplorer/Login.jsp  http://10.182.20.42:8102/uddiexplorer/Login.jsp  http://10.182.20.38:9202/uddiexplorer/Login.jsp  http://10.182.20.34:31002/uddiexplorer/Login.jsp  http://10.182.20.34:51007/uddiexplorer/Login.jsp  http://10.182.38.40:26001/uddiexplorer/Login.jsp  http://10.182.38.40:6001/uddiexplorer/Login.jsp  http://10.182.13.241:6001/uddiexplorer/Login.jsp  http://10.182.20.39:7002/uddiexplorer/Login.jsp  http://10.182.20.34:31005/uddiexplorer/Login.jsp  http://10.182.20.34:31001/uddiexplorer/Login.jsp  http://10.182.20.34:31003/uddiexplorer/Login.jsp  http://10.182.20.38:9105/uddiexplorer/Login.jsp  http://10.182.20.38:11001/uddiexplorer/Login.jsp  http://10.182.22.22:10001/uddiexplorer/Login.jsp  http://10.182.20.42:8104/uddiexplorer/Login.jsp  http://10.182.20.38:8094/uddiexplorer/Login.jsp  http://10.182.20.34:31006/uddiexplorer/Login.jsp  http://10.182.13.242:6001/uddiexplorer/Login.jsp  http://10.182.20.38:9203/uddiexplorer/Login.jsp  <http://10.182.20.38:9201/uddiexplorer/Login.jsp> | | |
| **漏洞验证** | http://10.182.20.42:11110/tomcat-docs/appdev/sample/web/hello.jsp?test=%3Cscript%3Ealert(12345)%3C/script%3E<script>39Da(9066)</script>    POST /uddiexplorer/SearchPublicRegistries.jsp HTTP/1.1  Content-Length: 160  Content-Type: application/x-www-form-urlencoded  Referer: http://10.182.20.38:8093/  Host: 10.182.20.38:8093  Connection: Keep-alive  Accept-Encoding: gzip,deflate  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21  Accept: \*/\*  btnSubmit=Search&operator='"()%26%25<acx><ScRiPt%20>alert(9920)</ScRiPt>&rdoSearch=name&selfor=Business%20location&txtSearchfor=&txtSearchkey=&txtSearchname=sdf | | |
| **整改建议** | 特殊字符转义，排查其它类似参数 | | |

* 1. [中危] CRLF注入

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | CRLF注入 | **风险级别** | 中 |
| **风险描述** | 攻击者能够控制HTTP 消息头中的字符，注入一些恶意的换行，以致于注入一些会话Cookie或者HTML代码。 | | |
| **漏洞URL** | http://10.182.13.241:6001  http://10.182.13.242:6001  http://10.182.13.243:6001  http://10.182.20.34:31001  http://10.182.20.34:31002  http://10.182.20.34:31003  http://10.182.20.34:31004  http://10.182.20.34:31005  http://10.182.20.34:31006  http://10.182.20.34:34007  http://10.182.20.34:51001  http://10.182.20.34:51007  http://10.182.20.34:8090  http://10.182.20.34:9001  http://10.182.20.38:11001  http://10.182.20.38:8081  http://10.182.20.38:8094  http://10.182.20.38:9101  http://10.182.20.38:9102  http://10.182.20.38:9103  http://10.182.20.38:9104  http://10.182.20.38:9105  http://10.182.20.38:9201  http://10.182.20.38:9202  http://10.182.20.38:9203  http://10.182.20.39:7002  http://10.182.20.39:9001  http://10.182.20.42:8102  http://10.182.20.42:8103  http://10.182.20.42:8104  http://10.182.20.42:9991  http://10.182.20.42:9996  http://10.182.21.51:7001  http://10.182.22.21:10001  http://10.182.22.22:10001  http://10.182.38.40:16001  http://10.182.38.40:26001  http://10.182.38.40:6001  http://10.185.22.188:6001  http://10.185.22.195:6001  <http://10.185.22.208:6001>  http://10.182.20.42:19003 | | |
| **漏洞验证** |  | | |
| **整改建议** | 过滤\r\n | | |

* 1. [中危] HOST头攻击

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | HOST头攻击 | **风险级别** | 中 |
| **风险描述** | HOST可能被恶意控制，可能导致缓存污染或者密码重置攻击。 | | |
| **漏洞URL** | http://10.182.13.241:6001  http://10.182.13.242:6001  http://10.182.13.243:6001  http://10.182.20.34:31001  http://10.182.20.34:31002  http://10.182.20.34:31003  http://10.182.20.34:31004  http://10.182.20.34:31005  http://10.182.20.34:31006  http://10.182.20.34:34007  http://10.182.20.34:51001  http://10.182.20.34:51007  http://10.182.20.34:8090  http://10.182.20.34:9001  http://10.182.20.38:11001  http://10.182.20.38:8081  http://10.182.20.38:8094  http://10.182.20.38:9101  http://10.182.20.38:9102  http://10.182.20.38:9103  http://10.182.20.38:9104  http://10.182.20.38:9105  http://10.182.20.38:9201  http://10.182.20.38:9202  http://10.182.20.38:9203  http://10.182.20.39:7002  http://10.182.20.39:9001  http://10.182.20.42:8102  http://10.182.20.42:8103  http://10.182.20.42:8104  http://10.182.20.42:9991  http://10.182.20.42:9996  http://10.182.21.51:7001  http://10.182.22.21:10001  http://10.182.22.22:10001  http://10.182.38.40:16001  http://10.182.38.40:26001  http://10.182.38.40:6001  http://10.185.22.188:6001  http://10.185.22.195:6001  <http://10.185.22.208:6001>  http://10.182.20.42:19003 | | |
| **漏洞验证** |  | | |
| **整改建议** | 判断host header的值 | | |

* 1. [高危] SVN信息泄露

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | SVN信息泄露 | **风险级别** | 高 |
| **风险描述** | SVN信息泄露，攻击者可能根据此漏洞获取网站敏感信息，可能包含源代码等其它敏感信息。 | | |
| **漏洞URL** | <http://10.182.20.43:8885/cas_web/.svn/entries>  <http://10.182.20.43:8885/cas_web/style/.svn/entries>  <http://10.182.20.43:8885/cas_web/js/.svn/entries> | | |
| **漏洞验证** |  | | |
| **整改建议** | 删除.svn目录或禁止访问此目录 | | |

* 1. [高危] Java调试线协议（Java Debug Wire Protocol）远程代码执行++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Java调试线协议（Java Debug Wire Protocol）远程代码执行 | **风险级别** | 高 |
| **风险描述** | 攻击者可以在未授权的情况下执行系统命令，从而获得目标服务器的控制权。 | | |
| **漏洞URL** | **http://172.20.35.39:8000** | | |
| **漏洞验证** |  | | |
| **整改建议** | 禁用Java调试线协议（Java Debug Wire Protocol） | | |

* 1. [中危] Hadoop集群敏感信息泄露++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Hadoop集群敏感信息泄露 | **风险级别** | 中 |
| **风险描述** | 存在Hadoop集群敏感信息泄露。 | | |
| **漏洞URL** | <http://172.20.35.45:8088/cluster>  <http://172.20.35.23:8088/cluster>  <http://172.20.32.23:8088/cluster>  172.20.50.36:8042  172.20.50.35:8042  172.20.50.34:8042  172.20.50.33:8042  172.20.50.32:8042  172.20.35.45:8042  172.20.35.24:8042  172.20.35.23:8042  172.20.32.99:8042  172.20.32.98:8042  172.20.32.97:8042  172.20.32.96:8042  172.20.32.95:8042  172.20.32.94:8042  172.20.32.93:8042  172.20.32.92:8042  172.20.32.91:8042  172.20.32.90:8042  172.20.32.89:8042  172.20.32.88:8042  172.20.32.87:8042  172.20.32.86:8042  172.20.32.85:8042  172.20.32.84:8042  172.20.32.83:8042  172.20.32.82:8042  172.20.32.81:8042  172.20.32.80:8042  172.20.32.79:8042  172.20.32.78:8042  172.20.32.77:8042  172.20.32.76:8042  172.20.32.75:8042  172.20.32.74:8042  172.20.32.73:8042  172.20.32.72:8042  172.20.32.71:8042  172.20.32.70:8042  172.20.32.111:8042  172.20.32.110:8042  172.20.32.109:8042  172.20.32.108:8042  172.20.32.107:8042  172.20.32.106:8042  172.20.32.105:8042  172.20.32.104:8042  172.20.32.103:8042  172.20.32.102:8042  172.20.32.101:8042  172.20.32.100:8042 | | |
| **漏洞验证** |  | | |
| **整改建议** | **授权访问** | | |

* 1. [高危] Zookeeper未授权访问++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Zookeeper未授权访问 | **风险级别** | 高 |
| **风险描述** | Zookeeper存在未授权访问，攻击者可通过执行envi命令获得系统大量的敏感信息，包括系统名称、Java环境等。 | | |
| **漏洞ip** | 172.20.35.49:2181  172.20.35.46:2181  172.20.35.44:2181  172.20.35.40:2181  172.20.35.23:2181  172.20.32.88:2181  172.20.32.87:2181  172.20.32.86:2181  172.20.32.85:2181  172.20.32.84:2181  172.20.32.83:2181  172.20.32.82:2181  172.20.32.81:2181  172.20.32.71:2181 | | |
| **漏洞验证** |  | | |
| **整改建议** | 添加访问控制，根据情况选择对应方式（认证用户，用户名密码，指定IP） | | |

* 1. [中危] FTP匿名访问++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | FTP匿名访问 | **风险级别** | 中 |
| **风险描述** | FTP存在匿名访问，可能导致数据泄露。 | | |
| **漏洞URL** | ftp://172.20.35.24 | | |
| **漏洞验证** |  | | |
| **整改建议** | 禁止匿名访问 | | |

* 1. [高危] MySQL弱口令++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | MySQL弱口令 | **风险级别** | 高 |
| **风险描述** | 攻击者可利用弱口令直接登录mysql数据库，上传恶意文件，从而获取系统权限或造成数据泄露 | | |
| **漏洞IP** | 172.20.35.48:3306  root/root | | |
| **漏洞验证** |  | | |
| **整改建议** | 修改弱口令，限制数据库外部访问 | | |

* 1. [高危] Hyperic HQ监控软件弱口令++

|  |  |  |  |
| --- | --- | --- | --- |
| **风险名称** | Hyperic HQ监控软件弱口令 | **风险级别** | 高 |
| **风险描述** | 攻击者可以进入管理后台，接管后台所有操作。 | | |
| **漏洞IP** | <http://172.20.32.22:17080/>  hqadmin/hqadmin | | |
| **漏洞验证** |  | | |
| **整改建议** | 修改弱口令 | | |