### 终端、业软互联网应用整改方法

对于终端、业软互联网应用的整改建议如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 弱点或漏洞描述 | 危害及后果 | 改进建议 | 风险等级 |
| 天天浏览器主站跨目录漏洞  showImg.action页面,imgpath使用文件路径作参数，存在跨目录问题 | 系统敏感文件及网站配置文件被读取 | 网站系统限制使用路径参数读取文件，而是应该使用ID值和路径的映射来索引一个文件 | 高 |
| 天天浏览器论坛后台弱密码漏洞  admin001的用户名密码相同 | 导致普通用可登陆网站后台，修改网站后台设置，上传webshell，控制网站 | 修改网站后台管理员帐号密码，后台管理员帐号密码不应该使用明文直接存放咋配置文件中 | 高 |
| 天天浏览器论坛后台文件上传漏洞  附件上传类型修改功能可以设置前台上传JSP文件 | 允许上传JSP类型文件导致可以上传恶意的JSP，形成WEBSHELL，完全控制网站 | 限制JSP等类型文件的上传 | 高 |
| 天天浏览器站点群应用服务器弱密码:  113.106.73.208:8080  TOMCAT管理控制中心  admin用户密码为admin | 匿名用户可以登陆tomcat后台，部署含有JSP木马的war包，获得网站webshell，控制网站服务器 | 关闭Tomcat后台管理页，或修改tomcat后台管理页默认帐号密码 | 高 |
| 天天空间跨站脚本漏洞  用户资料录入页面存在跨站脚本 | 录入恶意脚本可以危害其他用户 | 对录入内容中的特殊字符进行转义，包括<>’”等 | 高 |
| 天天装机必备网站跨目录漏洞  downloadPackege页面savefilename参数使用文件路径，存在跨目录问题 | 系统敏感文件及网站配置文件被读取 | 网站系统限制使用路径参数读取文件，而是应该使用ID值和路径的映射来索引一个文件 |  |
| 天天浏览器站点群服务器对公网开放高危端口 | 22，21等高危端口直接对公网开放容易造成黑客对网站服务器进行管理控制 | 修改防火墙策略，关闭高危端口 | 高 |
| 天天浏览器站点群应用服务器运行用户配置为ROOT权限 | 导致网站用户可以以ROOT权限访问系统 | 应该配置为NOBODY权限 | 高 |
| 终端BBS网站跨目录漏洞  index.php页面mod,app,type等参数均支持文件路径，导致跨目录问题 | 系统敏感文件及网站配置文件被读取 | 网站系统限制使用路径参数读取文件，而是应该使用ID值和路径的映射来索引一个文件 | 高 |
| [广告空间](http://www.adkongjian.com)网站跨目录漏洞  app.php页面m参数支持文件路径，导致跨目录的问题 | 系统敏感文件及网站配置文件被读取 | 网站系统限制使用路径参数读取文件，而是应该使用ID值和路径的映射来索引一个文件 | 高 |
| 终端云网站hicloud.com对用户录入的任何内容均无处理，导致跨站脚本问题 | 录入恶意脚本可以危害其他用户 | 对录入内容中的特殊字符进行转义，包括<>’”等 | 高 |
| 智汇云网站多个安全漏洞 | 1. 外网匿名用户可以使用任意密码登录网站管理后台，获得网站管理员权限  2. 外网匿名用户可以使用弱密码登录数据卡采集服务器管理后台，获得后台管理员权限  3. 外网匿名用户可以获得开发者论坛企业用户的明文密码和加密后的md5 hash，从而伪装受可信的企业用户发布APP程序 | 1. 修改网站管理后台权限验证设计逻辑；禁止网站管理后台对外网开放；  2. 使用复杂度高的登录密码；禁止管理后台对外网开放；  3. 存在密码泄露漏洞的页面属于网站内部逻辑，应屏蔽用户对这些页面的访问； | 高 |
| 业软互联网办公环境互联网出口NAT的测试环境存在多个应用服务器管理控制台弱密码  并且开启了多个高危端口 | 可利用测试环境作为跳板渗透入内网，盗取代码、数据等信息 | 禁止测试环境和高危端口对互联网的开放 | 高 |