# 漏洞概要

关注数(24) 关注此漏洞

缺陷编号：**wooyun-2012-010453**
漏洞标题：69个高校正方教务管理系统数据库任意操作
相关厂商：**正方教务管理系统**
漏洞作者：**独孤城**
提交时间：2012-08-01 16:36
修复时间：2012-09-15 16:37
公开时间：2012-09-15 16:37
漏洞类型：设计缺陷/逻辑错误
危害等级：高
自评Rank：10
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：

2012-08-01：细节已通知厂商并且等待厂商处理中
2012-08-06：厂商已经确认，细节仅向厂商公开
2012-08-16：细节向核心白帽子及相关领域专家公开
2012-08-26：细节向普通白帽子公开
2012-09-05：细节向实习白帽子公开
2012-09-15：细节向公众公开

简要描述：

如漏洞所描述，http://wooyun.org/bugs/wooyun-2010-010358，提交69个有漏洞的教务管理系统，任意数据库操作。

详细说明：

根据C/S服务器端口211检测，并使用本人编写的杭州正方漏洞说明工具软件检测，以下69所高校ＩＰ均存在数据库任意操作漏洞

```
60.21.206.169
jwgl.gdut.edu.cn
218.198.176.91
jwxt.jit.edu.cn
xfz.xaut.edu.cn
218.75.208.58
jw.tjrac.edu.cn
210.45.128.31
211.80.183.5
xk3.henu.edu.cn
58.193.0.26
xfz.xaut.edu.cn
202.201.106.24
jw.tlu.edu.cn
jwxt.zttc.edu.cn
jwglxt.buu.edu.cn
jwc.njty.edu.cn
jxgl.jsjzi.edu.cn
jwgl.xjvu.edu.cn
jwc.xust.edu.cn
jw.gzhtcm.edu.cn
jwxt.swun.edu.cn
211.82.16.106
202.200.144.63
202.203.31.97
202.116.160.167
210.44.128.152
210.38.111.227
202.200.112.200
jwgl.sias.edu.cn
202.194.250.254
210.44.159.3
210.44.159.2
jwgl.scce.edu.cn
202.199.155.2
61.180.31.37
218.196.207.8
116.236.150.101
218.9.77.221
210.45.98.13
222.30.226.20
202.116.160.166
219.159.198.146
211.103.139.211
219.245.6.246
210.44.159.6
222.19.168.156
219.159.199.85
202.121.31.23
218.107.191.119
210.36.200.6
wsxk.hbue.edu.cn
211.80.183.7
114.214.80.44
61.138.78.59
tas1.tjfsu.edu.cn
211.80.183.6
202.201.29.197
218.93.117.89
jwgl.fjzs.edu.cn
222.249.131.108
210.28.190.36
202.4.152.131
222.240.174.98
58.42.243.32
221.12.26.156
222.216.5.250
ce.jlu.edu.cn
61.180.31.37
```

漏洞证明：


同类型漏洞[ 设计缺陷/逻辑错误 ]：(10)

▼ 海尔旗下日日顺一处让人哭笑不得的奇葩设计
▼ ThinkPHP存储型XSS漏洞一枚
▼ 我是如何让女神从回我视线（绕过百度网盘关键字屏蔽下AV）
▼ 豆瓣某API扫号和暴力破解的问题
▼ 联想商城订单泄漏(包含姓名 手机号码 具体寄送地址等等)
▼ 好利网APP越权登录任意用户+越权获取全站几十万用户信息（密码md5\手机号\身份证\姓名\账户余额\银行卡）
▼ 海尔商城订单泄漏（包含姓名 手机号码 具体寄送地址等等）
▼ P2P安全之新新贷设计缺陷可重置任意用户密码（涉及用户资金安全）
▼ 畅途网某接口设计缺陷可撞库用户（泄漏用户信息）
▼ 网通营业厅客户信息泄露、充值支付价格修改漏洞

查看更多>>

同厂商漏洞[ 正方教务管理系统 ]：(10)

• 任意获取正方教务管理系统账号密码漏洞
• 正方教务系统低版本爆提权漏洞
• 正方教务管理系统读取学生头像注入漏洞
• 69个高校正方教务管理系统数据库任意操作

查看更多>>

同作者漏洞[ 独孤城 ]：(10)

◂ 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）
◂ 69个高校正方教务管理系统数据库任意操作
◂ 遵义市商业银行网站struts2漏洞

查看更多>>

随机漏洞展示：(8)

★ 暴风影音某站点一处存储型xss
★ 企慧通在线考试系统sql注入
★ 某情侣应用登陆未做限制可撞库
★ 金地集团官网SQL注入
★ 信托安全之渤海国际信托某站漏洞漏洞导致Getshell(涉及多系统数据库影响内网安全)
★ 福建招标与采购网分站存在注入漏洞
★ emlog设计缺陷可导致泄露数据库
★ 方正集团某处sql注入可执行系统命令（域权限）
★ Iwebsns sql 第一枚。
★ 中国电信某综合办公系统弱口令显示可无限制发送短信

查看更多>>


只检测一所高校来证明

修复方案：

由于C/S服务端使用的是Delphi的远程数据库组件，每台服务器的数据库连接认证应该修改，而不应该每个高校的服务器认证过程一样。



## 漏洞回应

厂商回应：

危害等级：高

漏洞Rank：20

确认时间：2012-08-06 08:23

厂商回复：

CNVD确认漏洞情况（部分复现），按通用软件漏洞评分原则(弥补一下上次忽略的分数)，rank 20

最新状态：

暂无