

漏洞概要

关注数(24) [关注此漏洞](#)缺陷编号: [wooyun-2012-010358](#)

漏洞标题: 正方教务管理系统数据库任意操作漏洞

相关厂商: 杭州正方

漏洞作者: 嵇麟君edwardz

提交时间: 2012-07-30 12:02

修复时间: 2012-08-04 12:03


公开时间: 2012-08-04 12:03

漏洞类型: 默认配置不当

危害等级: 高

自评Rank: 20

漏洞状态: 已由第三方合作机构(ncnrt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.orgTags标签: [无](#)分享漏洞:    4人收藏 

漏洞详情

披露状态:

2012-07-30: 细节已通知厂商并且等待厂商处理中

2012-08-04: 厂商已经主动忽略漏洞, 细节向公众公开

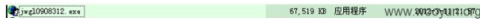
简要描述:

存在数据库任意操作漏洞, 只需要知道服务器IP, 可执行任意数据库操作, 因为全国1000多所高校都在使用该系统, 该漏洞可以直接实现成绩修改, 学生信息导出, 故影响十分严重且严重。

详细说明:

杭州正方教务管理系统是国内用的比较多的一个教务管理系统, 据杭州正方官网http://www.zfsoft.com/type_14.html 说正数字化校园信息平台软件用户名单 (共三十个省、市、自治区1000多所高校), 因此这个漏洞危害和影响还是相当大的。

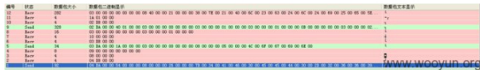
正方软件股份有限公司开发的教务管理系统除了.net 开发的B/S供学生查看成绩, 选课, 老师录入成绩以外, 还采用Delphi开发了一个C/S客户端, 用于教务员和老师排课改成绩等软件截图如下。



然而通过分析发现该软件存在许多重大漏洞, 用户只要知道了服务器IP, 就可以管理整个后台Oracle数据库, 导致学生老师的个人隐私信息泄露, 以及被篡改成绩的可能。而且经过我们的测试发现许多C/S服务端和B/S服务端在同一个服务器上, 比如218.75.208.58(湖南工业大学), 202.116.160.167(华南农业大学), 如果两个服务端不在同一个服务器上, 也比较好找, 因为C/S服务端使用的端口是211, 因此很容易通过端口扫描软件扫描整个C段或临近的网段找到服务器IP。

漏洞原理解析

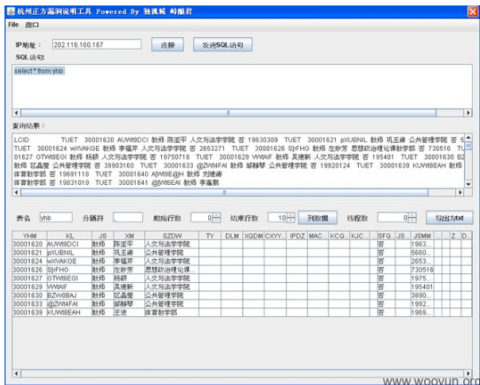
我们通过对客户端软件和服务端通信抓包过程发现, 每次打开客户端软件时, 客户端软件就跟服务器进行了三次TCP会话就完成了验证过程。经过我们的多次分析发现, 不管连接那台服务器, 这三次TCP会话都是固定的, 截图如下:



三次TCP会话后, 客户端就可以向服务端发送任意SQL语句了, 然后服务端就会返回查询结果。

SQL语句是这样构造的

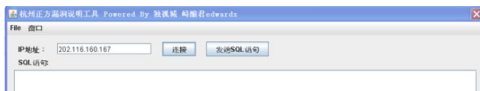
02DA0000+接下来数据的总字节数+030000000000000003000000022D310103000000010000000B000000FFFF030000000200000003000000000000000000000000+SQL语句的Unicode编码后的字节数+SQL的Unicode编码+080000000060000004000530050005F0071003100
发送给服务器后, 然后通过分析服务器就会返回数据包就可以得到返回的 S Q L 结果。



?

漏洞证明:

为了更好的说明漏洞的危害, 我们采用Java开发了漏洞说明软件, 并以华南农业大学(202.116.160.167)为例说明漏洞危害。



同类型漏洞[默认配置不当]: (10)

- ▼ 浙大恩特客户资源管理系统Boss远程代码执行导致的系统沦陷
- ▼ 乐视网SVN源码泄露, 可以读文件找漏洞
- ▼ Resin漏洞利用案例之目录遍历/以金蝶某系统为例
- ▼ 苏州电信光猫可通过VOIP接口进到邻家光猫
- ▼ 中兴通讯股份有限公司多款型号OLT设备存在安全风险
- ▼ 星星网站管理系统数据库下载
- ▼ 入侵中国移动自助营业厅终端
- ▼ EDayShop团购系统漏洞属之三#通用弱口令
- ▼ AVCON多媒体通信系统默认配置不当
- ▼ 金山毒霸企业版MongoDB配置不当存在安全隐患

[查看更多>>](#)

同厂商漏洞[杭州正方]: (10)

- ◆ 正方某通用型管理系统存在远程命令执行漏洞
- ◆ 正方教务系统未授权访问
- ◆ 杭州正方教务管理系统SQL注入漏洞, 可查询任意数据并附带exp
- ◆ 正方教务管理系统数据库任意操作漏洞
- ◆ 正方迎新管理系统漏洞命令执行
- ◆ 正方教务系统泄露学生信息
- ◆ 通用型正方教务 (通杀各版本) 存在注入 (不需登录) +获得webshell+提权内网漫游
- ◆ 正方教务管理系统漏洞XSS+过滤不严上传webshell
- ◆ 方正教务管理系统用户密码修改页面SQL注入漏洞
- ◆ 正方教务任意人的平时及考试成绩

[查看更多>>](#)

同作者漏洞[嵇麟君edwardz]: (10)

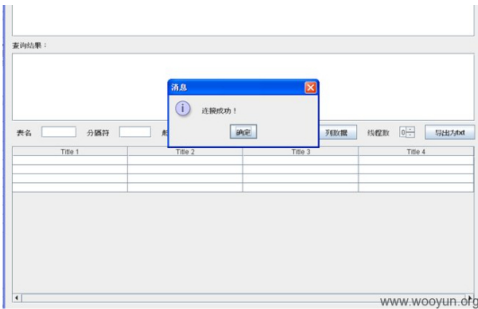
- ◆ 正方教务管理系统数据库任意操作漏洞

[查看更多>>](#)

随机漏洞展示: (8)

- ★ 酒仙网设计缺陷可绕过短信验证码支付密码和绑定的手机号码
- ★ 中兴某站存在用户弱口令导致敏感信息泄露
- ★ 武汉市某亮化监控系统弱口令 可控制路灯开关
- ★ 某伊份某系统部分员工存在弱口令可被外界进入
- ★ 中国东方航空某系统SQL注入 (stacked queries注入, 可跨34个库及数据)
- ★ tom某分站SQL注射导致getshell
- ★ 中国电信某分站远程执行命令
- ★ 爱丽网某分站存在注入漏洞
- ★ 快乐购网网某频道目录+注入
- ★ 广东联通悦特业务平台存在weblogic弱口令可shell

[查看更多>>](#)



将华南农业大学服务器IP输入IP地址栏后，点击连接，软件提示连接成功。



管理系统后台数据库里面有个表yhb,里面放着教师和管理的账户信息，包括加密后的密码。不过前段时间乌云报告了加密方式可逆的，很容易就能解密出来。输入SQL语句后，点击发送SQL语句。将返回查询结果，SQL语句可以是增删改查的其他任何符合Oracle的语句。

在表格里输入yhb,分隔符输入逗号，然后点击列数据，就可以看到查询数据了，并且可以导出为TXT。
通过上述说明，此漏洞确实很危险，感觉就像在裸奔一样，全国1000多所学校都在使用杭州正方教务管理系统，因此波及范围很广。
最后，欢迎关注微博：
<http://weibo.com/evilniang>
<http://weibo.com/bingobest>

修复方案：
通讯加密

版权声明：转载请注明来源 峙静君edwardz@乌云

漏洞回应

厂商回应：
危害等级：无影响厂商忽略
忽略时间：2012-08-04 12:03

厂商回复：
漏洞Rank: 20 (WooYun评价)

最新状态：
2012-08-04：关于近期正方教务系统出现的多个漏洞，CNVD目前处于批处理状态。由于处理不当导致本次白帽子提示的信息提前公开，致个歉。从目前处理情况看，已经初步完成事件情况确认。对漏洞事件评分按完全影响机密性评估，rank=7.79*1.3*1.5=15.190

