# 视频监控系统
# 信息安全检查报告

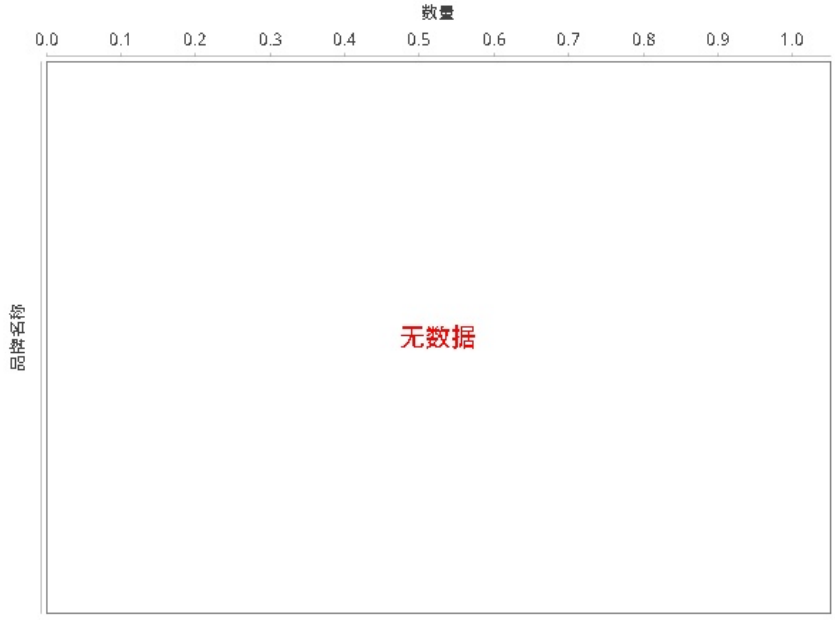
项目名：14
任务编号：1
检查日期：2019.07.06
检查人员：admin

技术支持中国科学院信息工程研究所

# 1.综合分析

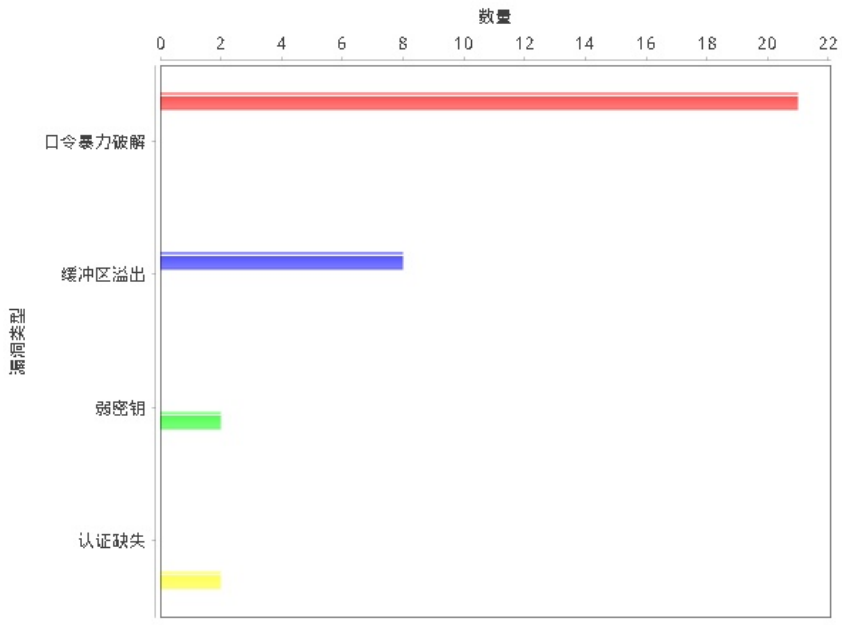
本次检查共发现33台存活主机。经深度检测分析，33个存活主机中工控设备0台，其他设备33台。工控设备中，具体分布如图1。

**图1 工控设备品牌分布**



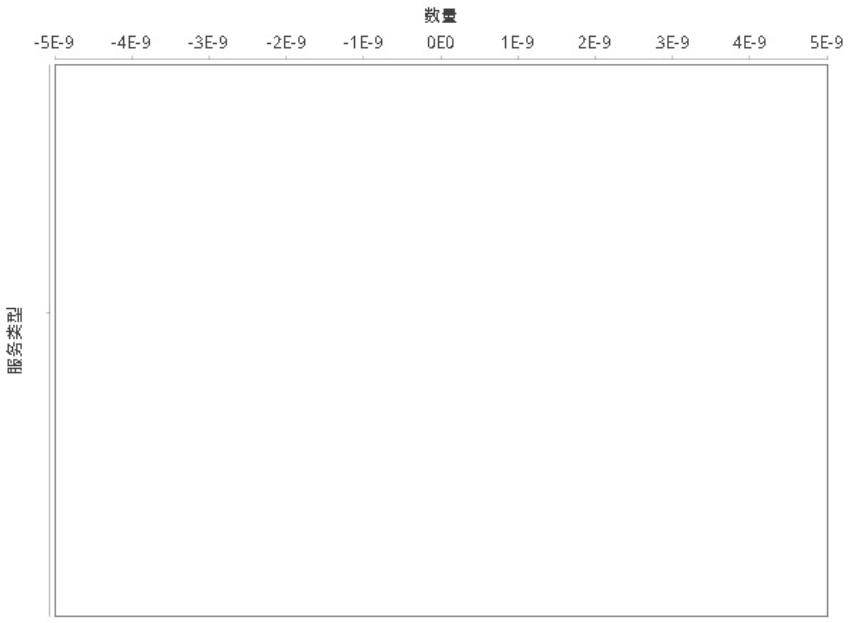

本次检查共发现漏洞33个，其中33个已验证，0个未验证，本地漏洞库扫描出33个，exploit扫描出0个，openVAS扫描出0个。存在漏洞的主机21台，占比63.64%。存在漏洞的工控设备0台，占比0。所有漏洞中，口令暴力破解21个，缓冲区溢出8个，弱密钥2个，认证缺失2个，具体分布如图2。

**图2 漏洞类型分布**




本次检查共识别出工控服务0个。

# 图3 工控服务分布



# 2.设备详情

表1 设备详情表

| 编号 | IP | 品牌 | 操作系统 | 协议服务 | 漏洞名称 | 漏洞等级 | 是否验证 | 来源 |
|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.14.1 | | Comware | ssh，tcp，22 | 无 | N/A | N/A | N/A |
| 2 | 192.168.14.57 | | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 3 | 192.168.14.58 | Hikvision | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | ssh，tcp，22 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 4 | 192.168.14.55 | | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 5 | 192.168.14.77 | | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 6 | 192.168.14.56 | | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 7 | 192.168.14.78 | GeoVision | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | snet-sensor-mgmt，tcp，10000 | 无 | N/A | N/A | N/A |
| 8 | 192.168.14.53 | Canon | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | ftp，tcp，21 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 9 | 192.168.14.75 | Vivotek | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | ftp，tcp，21 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-proxy，tcp，8080 | 无 | N/A | N/A | N/A |
| 10 | 192.168.14.76 | Vivotek | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | ftp，tcp，21 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-proxy，tcp，8080 | 无 | N/A | N/A | N/A |
| 11 | 192.168.14.51 | Suzhou Keda Technology CO. | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | ssh，tcp，22 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 12 | 192.168.14.73 | | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| 13 | 192.168.14.52 | Samsung | Linux | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 14 | 192.168.14.250 | | Linux | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| | | | | mysql，tcp，3306 | 无 | N/A | N/A | N/A |
| 15 | 192.168.14.50 | YAAN | Linux | onvif，tcp，85 | ONVIF验证缺失 | 高危 | 已验证 | 本地漏洞库 |
| | | | | | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 16 | 192.168.14.110 | Uniview | Linux | onvif，tcp，82 | 无 | N/A | N/A | N/A |
| | | | | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | DNP3，tcp，20000 | 无 | N/A | N/A | N/A |
| 17 | 192.168.14.112 | Uniview | Linux | onvif，tcp，81 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | hosts2-ns，tcp，81 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 18 | 192.168.14.49 | Hikvision | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 19 | 192.168.14.46 | Panasonic | embedded | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 20 | 192.168.14.68 | Uniview | Linux | onvif，tcp，80 | ONVIF弱密钥漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | hosts2-ns，tcp，81 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 21 | 192.168.14.47 | | Linux | onvif，tcp，80 | ONVIF验证缺失 | 高危 | 已验证 | 本地漏洞库 |
| | | | | | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 22 | 192.168.14.66 | Dahua | Linux | onvif，tcp，80 | ONVIF弱密钥漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | ssh，tcp，22 | 无 | N/A | N/A | N/A |
| | | | | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rpcbind，tcp，111 | 无 | N/A | N/A | N/A |
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 23 | 192.168.14.88 | TVT | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 24 | 192.168.14.45 | TRENDnet | Linux | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| 25 | 192.168.14.67 | | Linux | onvif，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| 26 | 192.168.14.64 | Hikvision | Linux | onvif，tcp，80 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | ssh，tcp，22 | 无 | N/A | N/A | N/A |
| | | | | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | RTSP 缓冲区溢出漏洞 | 高危 | 已验证 | 本地漏洞库 |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 27 | 192.168.14.108 | Beijing Hanbang Technology | Linux | onvif，tcp，8888 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | sun-answerbook，tcp，8888 | 无 | N/A | N/A | N/A |
| 28 | 192.168.14.43 | Hangzhou Zenointel Technology CO. | Linux | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | http-alt，tcp，8000 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 29 | 192.168.14.62 | Uniview | Linux | onvif，tcp，81 | ONVIF 暴力破解用户名密码漏洞 | 低危 | 已验证 | 本地漏洞库 |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | hosts2-ns，tcp，81 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 30 | 192.168.14.60 | Zavio | Linux | onvif，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 31 | 192.168.14.61 | | Linux | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| 32 | 192.168.14.80 | AXIS | Linux | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | https，tcp，443 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |
| 33 | 192.168.14.144 | AXIS | Linux | ftp，tcp，21 | 无 | N/A | N/A | N/A |
| | | | | telnet，tcp，23 | 无 | N/A | N/A | N/A |
| | | | | http，tcp，80 | 无 | N/A | N/A | N/A |
| | | | | rtsp，tcp，554 | 无 | N/A | N/A | N/A |
| | | | | unknown，tcp，49152 | 无 | N/A | N/A | N/A |

# 3.漏洞详情

表2 漏洞详情表

| 漏洞来源 | 漏洞名称 | 等级 | 设备IP | 是否验证 |
|---|---|---|---|---|
| 本地漏洞库 | ONVIF弱密钥漏洞 | 高危 | 192.168.14.57 | 已验证 |
| | | | 192.168.14.57 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.77 | 已验证 |
| | | | 192.168.14.56 | 已验证 |
| | | | 192.168.14.78 | 已验证 |
| | | | 192.168.14.53 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.51 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.112 | 已验证 |
| | | | 192.168.14.49 | 已验证 |
| | | | 192.168.14.49 | 已验证 |
| | | | 192.168.14.68 | 已验证 |
| | | | 192.168.14.68 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.88 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.108 | 已验证 |
| | | | 192.168.14.62 | 已验证 |
| | RTSP 缓冲区溢出漏洞 | 高危 | 192.168.14.57 | 已验证 |
| | | | 192.168.14.57 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.77 | 已验证 |
| | | | 192.168.14.56 | 已验证 |
| | | | 192.168.14.78 | 已验证 |
| | | | 192.168.14.53 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.51 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.112 | 已验证 |
| | | | 192.168.14.49 | 已验证 |
| | | | 192.168.14.49 | 已验证 |
| | | | 192.168.14.68 | 已验证 |

| | | | | |
|---|---|---|---|---|
| | | | 192.168.14.68 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.88 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.108 | 已验证 |
| | | | 192.168.14.62 | 已验证 |
| | ONVIF验证缺失 | 高危 | 192.168.14.57 | 已验证 |
| | | | 192.168.14.57 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.77 | 已验证 |
| | | | 192.168.14.56 | 已验证 |
| | | | 192.168.14.78 | 已验证 |
| | | | 192.168.14.53 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.51 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.112 | 已验证 |
| | | | 192.168.14.49 | 已验证 |
| | | | 192.168.14.49 | 已验证 |
| | | | 192.168.14.68 | 已验证 |
| | | | 192.168.14.68 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.88 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.108 | 已验证 |
| | | | 192.168.14.62 | 已验证 |
| | ONVIF 暴力破解用户名密码漏洞 | 低危 | 192.168.14.57 | 已验证 |
| | | | 192.168.14.57 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.58 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.55 | 已验证 |
| | | | 192.168.14.77 | 已验证 |
| | | | 192.168.14.56 | 已验证 |
| | | | 192.168.14.78 | 已验证 |
| | | | 192.168.14.53 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.75 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.76 | 已验证 |
| | | | 192.168.14.51 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.73 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.50 | 已验证 |
| | | | 192.168.14.112 | 已验证 |
| | | | 192.168.14.49 | 已验证 |

| | | | | |
|---|---|---|---|---|
| | | | 192.168.14.49 | 已验证 |
| | | | 192.168.14.68 | 已验证 |
| | | | 192.168.14.68 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.47 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.66 | 已验证 |
| | | | 192.168.14.88 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.64 | 已验证 |
| | | | 192.168.14.108 | 已验证 |
| | | | 192.168.14.62 | 已验证 |