# 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

## 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。

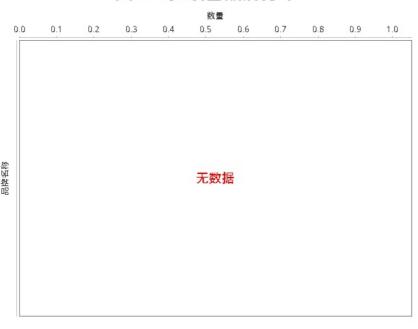
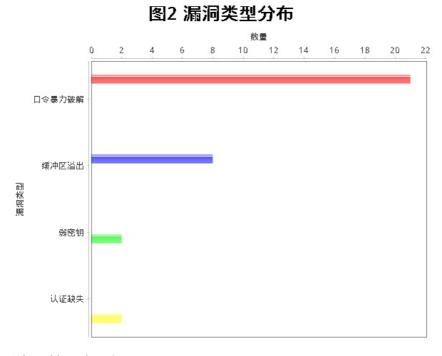


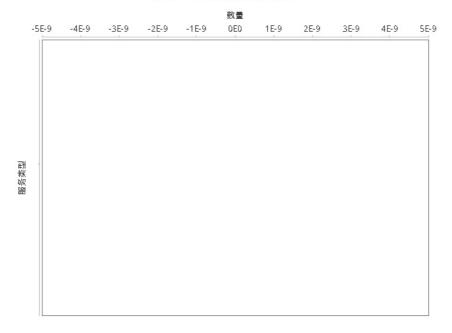
图1 工控设备品牌分布

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。



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
				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
2	192.168.14.57		Linux	http- alt,tcp,8000	无	N/A	N/A	N/A
				unknown, tcp , 49152	无	N/A	N/A	N/A
				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
3	192.168.14.58	Hikvision	Linux	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
	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
4				http- alt,tcp,8000	无	N/A	N/A	N/A
				unknown, tcp , 49152	无	N/A	N/A	N/A
				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
5	192.168.14.77		Linux	http, tcp, 80	无	N/A	N/A	N/A
				rtsp, tcp, 554	无	N/A	N/A	N/A
				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
6	192.168.14.56		Linux	rtsp, tcp, 554	无	N/A	N/A	N/A
				unknown, tcp , 49152	无	N/A	N/A	N/A
				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
_	100 100 1 -	6		http, tcp, 80	无	N/A	N/A	N/A
7	192.168.14.78	GeoVision	Linux	snet-sensor- mgmt, tcp, 1 0000	无	N/A	N/A	N/A
				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
8	192.168.14.53	Canon	Linux	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
				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 无	N/A	N/A	N/A
				http, tcp, 80	无	N/A	N/A	N/A
9	192.168.14.75	Vivotek	Linux	rtsp, tcp, 554	RTSP 缓冲区溢出漏洞	 高危	已验证	本地漏洞库
				http- proxy, tcp, 80 80	无	N/A	N/A	N/A
				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
10	192.168.14.76	Vivotek	Linux	rtsp, tcp, 554	RTSP 缓冲区溢出漏洞	高危	已验证	本地漏洞库
				http- proxy, tcp, 80 80	无	N/A	N/A	N/A
				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
11	102 100 14 51	Suzhou Keda	Limene	ssh, tcp, 22	无	N/A	N/A	N/A
11	192.168.14.51	Technology CO.	Linux	http, tcp, 80	无	N/A	N/A	N/A
				rtsp, tcp, 554	无	N/A	N/A	N/A
			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
		3		http, tcp, 80	无	N/A	N/A	N/A
12	192.168.14.73			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
		Samsung	Linux	http, tcp, 80	无	N/A	N/A	N/A
13	192.168.14.52			https, tcp, 44	无	N/A	N/A	N/A
10	132.100.11.32		Lillax	rtsp, tcp, 554	无	N/A	N/A	N/A
				unknown, tcp , 49152	无	N/A	N/A	N/A
				http, tcp, 80	无	N/A	N/A	N/A
14	192.168.14.250		Linux	https, tcp, 44	无	N/A	N/A	N/A
				mysql, tcp, 3	无	N/A	N/A	N/A
				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
15	192.168.14.50	YAAN	Linux	telnet, tcp, 2	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
				onvif, tcp, 82	无	N/A	N/A	N/A
16	192.168.14.110	Uniview	Linux	telnet, tcp, 2	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, 20	无	N/A	N/A	N/A
				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
17	192.168.14.112	Uniview	Linux	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
				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, 44	无	N/A	N/A	N/A
18	192.168.14.49	Hikvision	Linux	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
10	102 100 14 40	Danasania	0.000 0.00 0.00	http, tcp, 80	无	N/A	N/A	N/A
19	192.168.14.46	Panasonic	embedded	rtsp, tcp, 554	无	N/A	N/A	N/A
		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
20	192.168.14.68			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
				onvif, tcp, 80	ONVIF验证缺失	高危	已验证	本地漏洞库
				onvii, tcp, 80	ONVIF 暴力破解用户名密码漏洞	低危	已验证	本地漏洞库
21	192.168.14.47		Linux	telnet, tcp, 2	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
				onvif, tcp, 80	ONVIF弱密钥漏洞	高危	已验证	本地漏洞库
				опин, тер, оо	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, 2	无	N/A	N/A	N/A
22	102 160 14 66	Dahua	Linux	http, tcp, 80	无	N/A	N/A	N/A
ZZ	192.168.14.66	Dahua	Linux	rpcbind, tcp, 111	无	N/A	N/A	N/A
				https, tcp, 44	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

		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
23	192.168.14.88			http, tcp, 80	无	N/A	N/A	N/A
				rtsp, tcp, 554	无	N/A	N/A	N/A
	100 100 14 45	TOFNE		http, tcp, 80	无	N/A	N/A	N/A
24	192.168.14.45	TRENDnet	Linux	https, tcp, 44	无	N/A	N/A	N/A
				onvif, tcp, 80	无	N/A	N/A	N/A
				http, tcp, 80	无	N/A	N/A	N/A
25	192.168.14.67		Linux	rtsp, tcp, 554	无	N/A	N/A	N/A
				http- alt, tcp, 8000	无	N/A	N/A	N/A
				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, 2	无	N/A	N/A	N/A
				http, tcp, 80	无	N/A	N/A	N/A
26	192.168.14.64	Hikvision	Linux	https, tcp, 44	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
		Beijing Hanbang Technology	Linux	onvif, tcp, 88	ONVIF 暴力破解用户名密码漏洞	低危	已验证	本地漏洞库
	192.168.14.108			telnet, tcp, 2	无	N/A	N/A	N/A
27				http, tcp, 80	无	N/A	N/A	N/A
				sun- answerbook, t cp, 8888	无	N/A	N/A	N/A
				telnet, tcp, 2	无	N/A	N/A	N/A
		Hangzhou		http, tcp, 80	无	N/A	N/A	N/A
28	192.168.14.43	Hangzhou Zenointel Technology CO.	Linux	rtsp, tcp, 554	无	N/A	N/A	N/A
20	192.100.14.43		Liliux	http- alt, tcp, 8000	无	N/A	N/A	N/A
				unknown, tcp , 49152	无	N/A	N/A	N/A
				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
29	192.168.14.62	Uniview	Linux	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
20	102 162 14 62	7	1:	onvif, tcp, 80	无	N/A	N/A	N/A
30	192.168.14.60	Zavio	Linux	http, tcp, 80	无	N/A	N/A	N/A

				https, tcp, 44	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
31	192.108.14.01		LIIIux	rtsp, tcp, 554	无	N/A	N/A	N/A
		AXIS	Linux	http, tcp, 80	无	N/A	N/A	N/A
22	192.168.14.80			https, tcp, 44	无	N/A	N/A	N/A
32				rtsp, tcp, 554	无	N/A	N/A	N/A
				unknown, tcp , 49152	无	N/A	N/A	N/A
			Linux	ftp, tcp, 21	无	N/A	N/A	N/A
	192.168.14.144	AXIS		telnet, tcp, 2	无	N/A	N/A	N/A
33				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
			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
	ONVIF弱密钥漏洞	高危	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
本地漏洞库			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
			192.168.14.57	已验证
			192.168.14.57	已验证
			192.168.14.58	
			192.168.14.58	已验证
			192.168.14.55	
			192.168.14.55	
			192.168.14.77	
			192.168.14.56	已验证
			192.168.14.78	
			192.168.14.78	已验证
			192.168.14.75	已验证
	RTSP 缓冲区溢出漏洞	高危	192.168.14.75	
	11.01 级/T/区/皿山/網/円	同化	192.168.14.76	
			192.168.14.76	已验证
			192.168.14.76	已验证
				已验证
			192.168.14.73	
			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

			1	
			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
			192.168.14.57	已验证 已验证
			192.168.14.57 192.168.14.58	<u>已验证</u>
			192.168.14.58	已验证 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
	ONVIF验证缺失	高危	192.168.14.73	已验证
			192.168.14.50	
			192.168.14.50	
			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
			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
	ONVIF 暴力破解用户名密码漏洞	低危	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

192.168.14.4	9 已验证
192.168.14.6	8 已验证
192.168.14.6	8 已验证
192.168.14.4	7 已验证
192.168.14.4	7 已验证
192.168.14.6	6 已验证
192.168.14.6	6 已验证
192.168.14.8	8 已验证
192.168.14.6	4 已验证
192.168.14.6	4 已验证
192.168.14.10	08 已验证
192.168.14.6	2 已验证