视频监控系统
信息安全检查报告

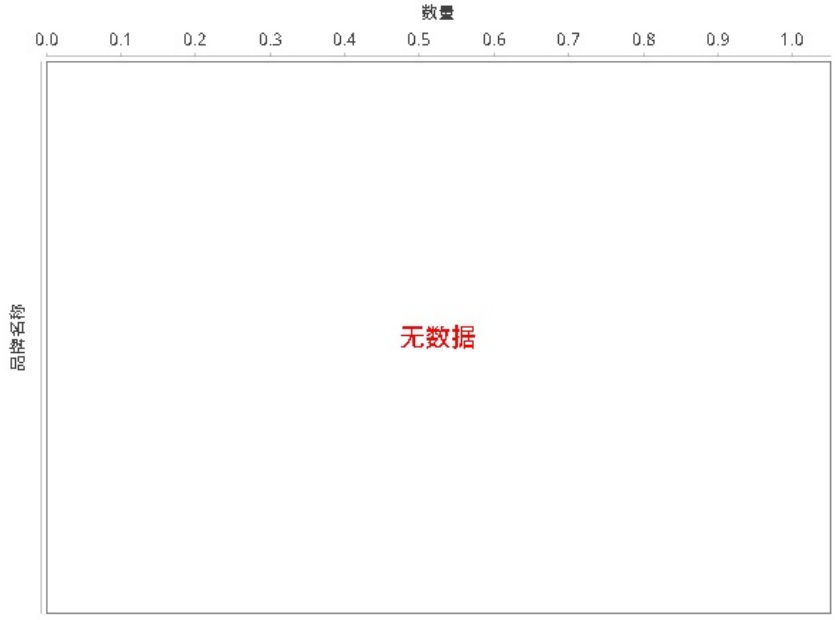
项目名：test
任务编号：1
检查日期：2019.07.11
检查人员：admin

技术支持中国科学院信息工程研究所

1.综合分析

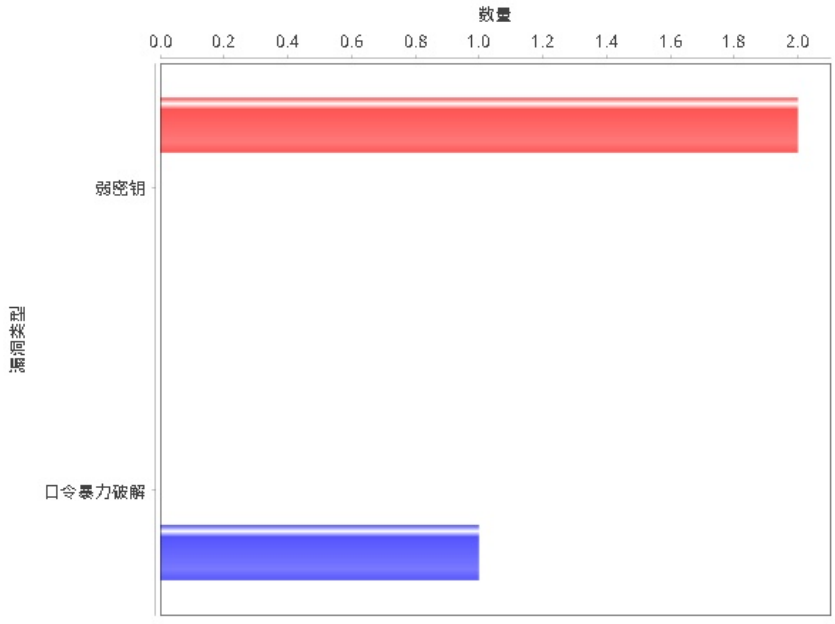
本次检查共发现66台存活主机。经深度检测分析，66个存活主机中工控设备0台，其他设备66台。工控设备中，具体分布如图1。

图1 工控设备品牌分布



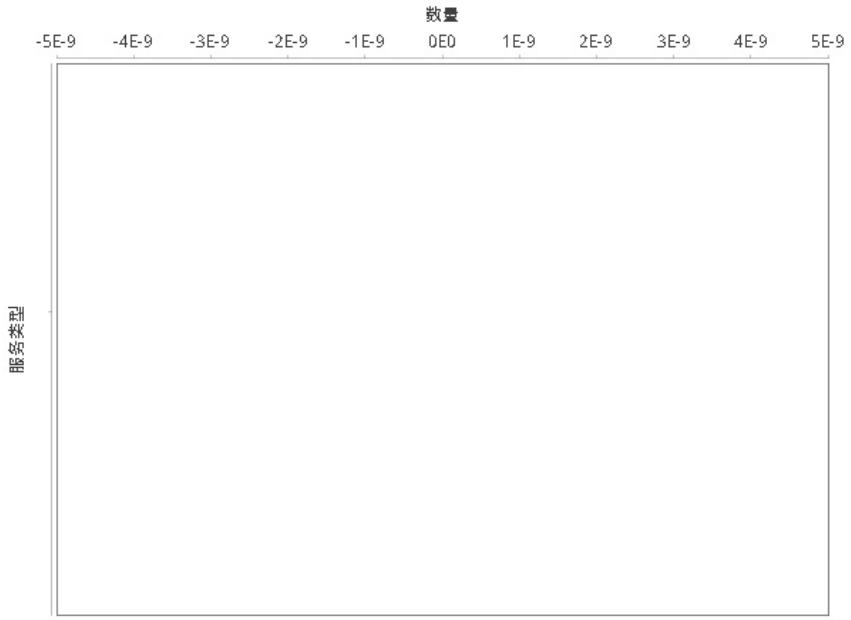
本次检查共发现漏洞3个，其中3个已验证，0个未验证，本地漏洞库扫描出3个，exploit扫描出0个，openVAS扫描出0个。存在漏洞的主机3台，占比4.55%。存在漏洞的工控设备0台，占比0。所有漏洞中，弱密钥2个，口令暴力破解1个，具体分布如图2。

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	10.10.12.90	Super Micro Computer	Linux	ssh，tcp，22	无	N/A	N/A	N/A
				http，tcp，80	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
				X11:1，tcp，6001	无	N/A	N/A	N/A
2	10.10.13.223		Linux	ssh，tcp，22	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
				mysql，tcp，3306	无	N/A	N/A	N/A

				http-proxy，tcp，8080	无	N/A	N/A	N/A
3	10.10.13.143		Windows	https，tcp，443	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
5	10.10.12.181	Dell	Linux	ssh，tcp，22	无	N/A	N/A	N/A
6	10.10.12.183	Universal Global Scientific Industrial Co.	Windows	https，tcp，443	无	N/A	N/A	N/A
				vnc，tcp，5900	无	N/A	N/A	N/A
7	10.10.12.98	Compal Information (kunshan) CO.	Windows	S7，tcp，102	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
9	10.10.13.66	Dell	Windows	mysql，tcp，3306	无	N/A	N/A	N/A
10	10.10.12.57	Universal Global Scientific Industrial Co.	Linux	rpcbind，tcp，111	无	N/A	N/A	N/A
				cisco-sccp，tcp，2000	无	N/A	N/A	N/A
12	10.10.12.95	Universal Global Scientific Industrial Co.	Windows	ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
13	10.10.12.135		Linux	ssh，tcp，22	无	N/A	N/A	N/A
14	10.10.13.112	Hewlett Packard	Linux	ssh，tcp，22	无	N/A	N/A	N/A
				rpcbind，tcp，111	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
				http-proxy，tcp，8080	无	N/A	N/A	N/A
15	10.10.12.81	Dell	Linux	ssh，tcp，22	无	N/A	N/A	N/A
				dc，tcp，2001	无	N/A	N/A	N/A
16	10.10.13.154		embedded	mysql，tcp，3306	无	N/A	N/A	N/A
17	10.10.12.82		Linux	ssh，tcp，22	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
18	10.10.13.152		Windows	https，tcp，443	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
19	10.10.13.153		Windows	https，tcp，443	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A

				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
20	10.10.13.56	Universal Global Scientific Industrial Co.	embedded	https，tcp，443	无	N/A	N/A	N/A
21	10.10.12.45		FreeBSD	https，tcp，443	无	N/A	N/A	N/A
22	10.10.12.89		Linux	ssh，tcp，22	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
23	10.10.12.83	Universal Global Scientific Industrial Co.	Linux	ssh，tcp，22	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
24	10.10.13.52	eac Automation-consulting Gmbh	Linux	ssh，tcp，22	无	N/A	N/A	N/A
				http，tcp，80	无	N/A	N/A	N/A
				http-alt，tcp，8000	无	N/A	N/A	N/A
25	10.10.12.203	Universal Global Scientific Industrial Co.	Windows	ftp，tcp，21	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
				LSA-or-nterm，tcp，1026	无	N/A	N/A	N/A
				IIS，tcp，1027	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
26	10.10.12.127		JUNOS	https，tcp，443	无	N/A	N/A	N/A
27	10.10.12.1	Huawei Technologies Co.	embedded	telnet，tcp，23	无	N/A	N/A	N/A
				snmp，udp，161	无	N/A	N/A	N/A
29	10.10.12.241		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
30	10.10.12.165	Universal Global Scientific Industrial Co.		https，tcp，443	无	N/A	N/A	N/A
31	10.10.12.123	Universal Global Scientific Industrial Co.	JUNOS	https，tcp，443	无	N/A	N/A	N/A
32	10.10.12.200	TP-Link	Windows	https，tcp，443	无	N/A	N/A	N/A
				vnc，tcp，5900	无	N/A	N/A	N/A

33	10.10.12.168		FreeBSD	http-alt，tcp，8000	无	N/A	N/A	N/A
34	10.10.12.201	Universal Global Scientific Industrial Co.	Windows	ftp，tcp，21	FTP服务弱密钥漏洞	高危	已验证	本地漏洞库
				https，tcp，443	无	N/A	N/A	N/A
				LSA-or-nterm，tcp，1026	无	N/A	N/A	N/A
				IIS，tcp，1027	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
35	10.10.13.201		Linux	ssh，tcp，22	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
				mysql，tcp，3306	无	N/A	N/A	N/A
36	10.10.13.165		Windows	https，tcp，443	无	N/A	N/A	N/A
37	10.10.13.164	Universal Global Scientific Industrial Co.	Windows	https，tcp，443	无	N/A	N/A	N/A
38	10.10.13.45	Dell	Windows	https，tcp，443	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
40	10.10.13.206		Linux	ssh，tcp，22	SSH服务弱密钥漏洞	高危	已验证	本地漏洞库
				mysql，tcp，3306	无	N/A	N/A	N/A
				http-proxy，tcp，8080	无	N/A	N/A	N/A
43	10.10.13.205	Universal Global Scientific Industrial Co.	Linux	ssh，tcp，22	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
				mysql，tcp，3306	无	N/A	N/A	N/A
46	10.10.12.198	Asix Electronics	Windows	https，tcp，443	无	N/A	N/A	N/A
				vnc，tcp，5900	无	N/A	N/A	N/A
49	10.10.13.70		Linux	ssh，tcp，22	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
				mysql，tcp，3306	无	N/A	N/A	N/A

50	10.10.13.212	eac Automation-consulting Gmbh	Linux	ssh，tcp，22	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
				mysql，tcp，3306	无	N/A	N/A	N/A
51	10.10.13.210	Anviz Biometric Tech. Co.	Linux	ssh，tcp，22	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
				http-proxy，tcp，8080	无	N/A	N/A	N/A
52	10.10.13.251	Kyland Technology Co.	Linux	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
53	10.10.12.192		Windows	https，tcp，443	无	N/A	N/A	N/A
				vnc，tcp，5900	无	N/A	N/A	N/A
54	10.10.13.173	Universal Global Scientific Industrial Co.	Windows	https，tcp，443	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
55	10.10.13.250	GE	Windows	http，tcp，80	无	N/A	N/A	N/A
				LSA-or-nterm，tcp，1026	无	N/A	N/A	N/A
				IIS，tcp，1027	无	N/A	N/A	N/A
				ms-wbt-server，tcp，3389	无	N/A	N/A	N/A
58	10.10.13.36	Lcfc(hefei) Electronics Technology co.	Windows	https，tcp，443	无	N/A	N/A	N/A
				rtsp，tcp，554	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
59	10.10.13.213	eac Automation-consulting Gmbh	Linux	ssh，tcp，22	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
61	10.10.13.214	eac Automation-consulting Gmbh	Linux	ssh，tcp，22	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
				mysql，tcp，3306	无	N/A	N/A	N/A

				http-proxy，tcp，8080	无	N/A	N/A	N/A
62	10.10.12.106	Universal Global Scientific Industrial Co.	Windows	S7，tcp，102	无	N/A	N/A	N/A
				https，tcp，443	无	N/A	N/A	N/A
64	10.10.13.3	Universal Global Scientific Industrial Co.	Windows	https，tcp，443	无	N/A	N/A	N/A
				rtsp，tcp，554	无	N/A	N/A	N/A
				mysql，tcp，3306	无	N/A	N/A	N/A
66	10.10.12.147		Linux	ssh，tcp，22	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	FTP服务弱密钥漏洞	高危	10.10.12.241	已验证
			10.10.12.201	已验证
			10.10.13.206	已验证
	SSH服务弱密钥漏洞	高危	10.10.12.241	已验证
			10.10.12.201	已验证
			10.10.13.206	已验证
	ONVIF 暴力破解用户名密码漏洞	低危	10.10.12.241	已验证
			10.10.12.201	已验证
			10.10.13.206	已验证