视频监控系统
信息安全检查报告

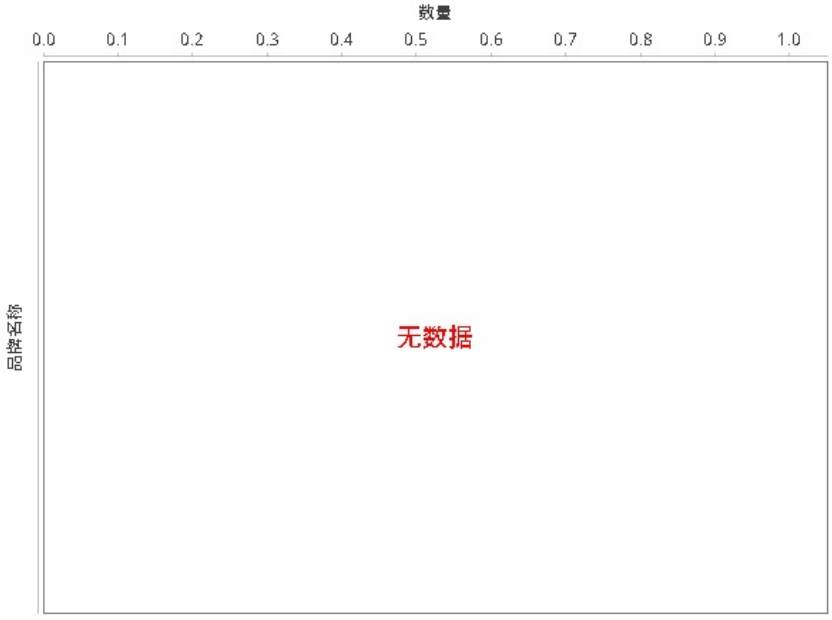
项目名：B13
任务编号：1
检查日期：2019.07.11
检查人员：admin

技术支持中国科学院信息工程研究所

1.综合分析

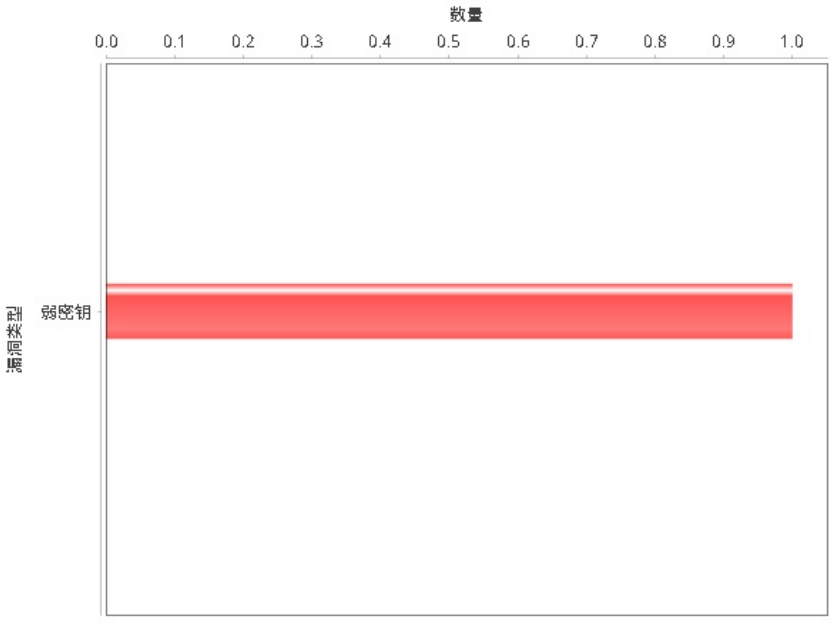
本次检查共发现30台存活主机。经深度检测分析，30个存活主机中工控设备0台，其他设备30台。工控设备中，具体分布如图1。

图1 工控设备品牌分布



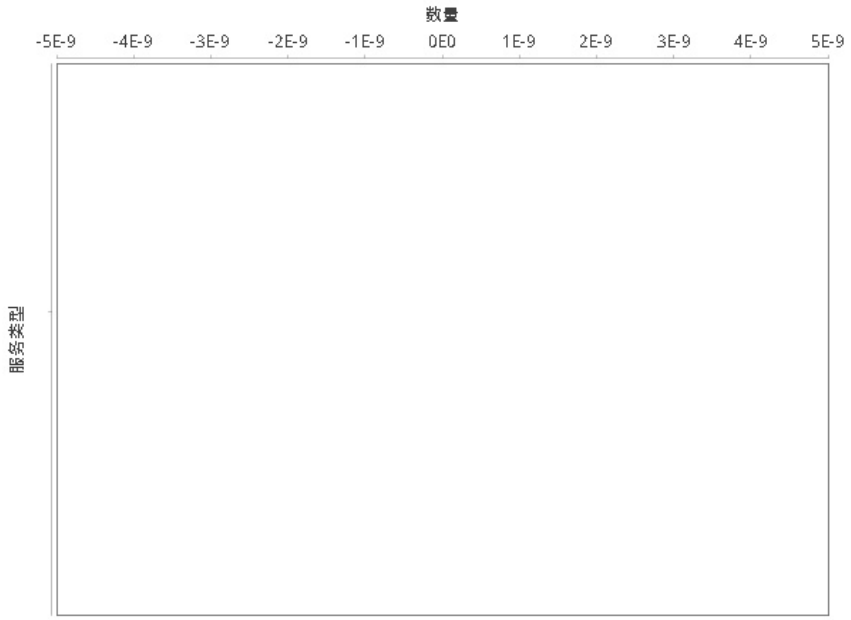
本次检查共发现漏洞1个，其中1个已验证，0个未验证，本地漏洞库扫描出1个，exploit扫描出0个，openVAS扫描出0个。存在漏洞的主机1台，占比3.33%。存在漏洞的工控设备0台，占比0。所有漏洞中，弱密钥1个，具体分布如图2。

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	10.10.13.201		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
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
4	10.10.13.165		Windows	https，tcp，443	无	N/A	N/A	N/A
5	10.10.13.164	Universal Global Scientific Industrial Co.	Windows	https，tcp，443	无	N/A	N/A	N/A
6	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
9	10.10.13.66	Dell	Windows	mysql，tcp，3306	无	N/A	N/A	N/A
10	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
14	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
15	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
16	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
17	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
18	10.10.13.154		embedded	mysql，tcp，3306	无	N/A	N/A	N/A

19	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
20	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
21	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
22	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
23	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
24	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
25	10.10.13.56	Universal Global Scientific Industrial Co.	embedded	https，tcp，443	无	N/A	N/A	N/A
26	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
27	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
28	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

29	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
30	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

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	SSH服务弱密钥漏洞	高危	10.10.13.206	已验证