

电力终端系统漏洞扫描报告

项目名：10.10.10.0/24

任务编号：2

检查日期：2019.07.23

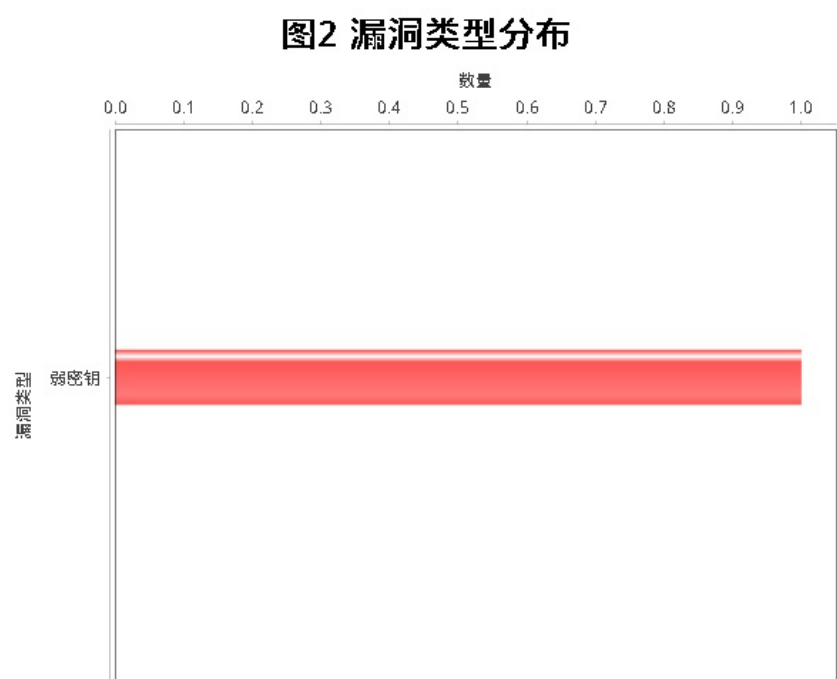
检查人员：admin

1.综合分析

本次检查共发现40台存活主机。经深度检测分析，40个存活主机中工控设备0台，其他设备40台。工控设备中，具体分布如图1。



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2.50%。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。



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	10.10.10.30	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
					无	N/A	N/A	N/A
3	10.10.10.32	Elitegroup Computer Systems Co.	FreeBSD	ms-wbt-server, tcp, 3389	无	N/A	N/A	N/A
4	10.10.10.54	Realtek Semiconductor	Windows	ssh, tcp, 22	无	N/A	N/A	N/A
5	10.10.10.76		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

6	10.10.10.11		Windows	https, tcp, 443	无	N/A	N/A	N/A
				ms-wbt-server, tcp, 3389	无	N/A	N/A	N/A
				http-proxy, tcp, 8080	无	N/A	N/A	N/A
				unknown, tcp, 49152	无	N/A	N/A	N/A
				unknown, tcp, 49154	无	N/A	N/A	N/A
					无	N/A	N/A	N/A
7	10.10.10.33	Lcfc(hefei) Electronics Technology Co.	Windows	http, tcp, 80	无	N/A	N/A	N/A
				https, tcp, 443	无	N/A	N/A	N/A
8	10.10.10.77	Le Shi Zhi Xin Electronic Technology (Tianjin) Co.	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
9	10.10.10.70		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
10	10.10.10.71	Mitac Technology	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
11	10.10.10.51	Realtek Semiconductor	iOS	domain, tcp, 53	无	N/A	N/A	N/A
12	10.10.10.18	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
13	10.10.10.12	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
				http-proxy, tcp, 8080	无	N/A	N/A	N/A
				unknown, tcp, 49152	无	N/A	N/A	N/A
				unknown, tcp, 49154	无	N/A	N/A	N/A

14	10.10.10.34	Elitegroup Computer Systems Co.	Windows	mysql, tcp, 3306	无	N/A	N/A	N/A
				ms-wbt-server, tcp, 3389	无	N/A	N/A	N/A
15	10.10.10.56	Lcfc(hefei) Electronics Technology co.	Linux	ssh, tcp, 22	无	N/A	N/A	N/A
				http, tcp, 80	无	N/A	N/A	N/A
16	10.10.10.35	Universal Global Scientific Industrial Co.	Windows	http, tcp, 80	无	N/A	N/A	N/A
				https, tcp, 443	无	N/A	N/A	N/A
				ms-wbt-server, tcp, 3389	无	N/A	N/A	N/A
				unknown, tcp, 49152	无	N/A	N/A	N/A
				unknown, tcp, 49154	无	N/A	N/A	N/A
17	10.10.10.79		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
18	10.10.10.14	Elitegroup Computer Systems Co.	Windows	ftp, tcp, 21	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	10.10.10.15	Universal Global Scientific Industrial Co.	Windows	ms-wbt-server, tcp, 3389	无	N/A	N/A	N/A
21	10.10.10.37	Dell	Windows	http, tcp, 80	无	N/A	N/A	N/A
				ms-wbt-server, tcp, 3389	无	N/A	N/A	N/A
				http-alt, tcp, 8000	无	N/A	N/A	N/A
23	10.10.10.242		Comware	ssh, tcp, 22	无	N/A	N/A	N/A
25	10.10.10.20	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
26	10.10.10.42	Universal Global Scientific Industrial Co.	Windows	http, tcp, 80	无	N/A	N/A	N/A
				ms-wbt-server, tcp, 3389	无	N/A	N/A	N/A
				http-alt, tcp, 8000	无	N/A	N/A	N/A

				http-proxy, tcp, 8080	无	N/A	N/A	N/A
					无	N/A	N/A	N/A
27	10.10.10.64	Lcfc(hefei) Electronics Technology co.	Linux	ssh, tcp, 22	SSH服务弱密钥漏洞	高危	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
				mysql, tcp, 3306	无	N/A	N/A	N/A
28	10.10.10.22	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
29	10.10.10.81	Tenda Technology Co.	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
31	10.10.10.1	Huawei Technologies Co.	embedded	telnet, tcp, 23	无	N/A	N/A	N/A
				snmp, udp, 161	无	N/A	N/A	N/A
32	10.10.10.27	G-pro Computer	Linux	ssh, tcp, 22	无	N/A	N/A	N/A
33	10.10.10.28		Linux	ssh, tcp, 22	无	N/A	N/A	N/A
34	10.10.10.23	Apple	iOS	ssh, tcp, 22	无	N/A	N/A	N/A
				http, tcp, 80	无	N/A	N/A	N/A
				afp, tcp, 548	无	N/A	N/A	N/A
35	10.10.10.5	TP-Link	embedded	telnet, tcp, 23	无	N/A	N/A	N/A
				snmp, udp, 161	无	N/A	N/A	N/A
36	10.10.10.67	Asix Electronics	iOS	domain, tcp, 53	无	N/A	N/A	N/A
				mysql, tcp, 3306	无	N/A	N/A	N/A
37	10.10.10.68		Windows	unknown, tcp, 49152	无	N/A	N/A	N/A
				unknown, tcp, 49154	无	N/A	N/A	N/A
38	10.10.10.25	Dell	FreeBSD	https, tcp, 443	无	N/A	N/A	N/A
				mysql, tcp, 3306	无	N/A	N/A	N/A
39	10.10.10.69	Lcfc(hefei) Electronics Technology co.	Windows	unknown, tcp, 49152	无	N/A	N/A	N/A
				unknown, tcp, 49154	无	N/A	N/A	N/A
40	10.10.10.210	HP	embedded	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
				https, tcp, 443	无	N/A	N/A	N/A
				printer, tcp, 515	无	N/A	N/A	N/A
				http-proxy, tcp, 8080	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	10.10.10.64	已验证