202409漏扫报告

报告时间：2024-09-13 12:44:45

1. 综述

1.1 任务信息

本次任务发现 22 个资产， 8 个存活ip， 22 个开放端口。 经详细分析，共有 0 个硬件产品， 1 个软件产品。

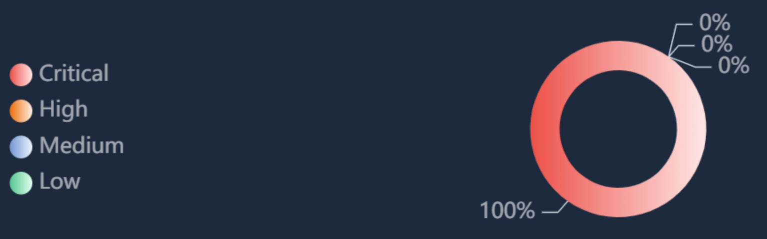
22	8	22	1	0	4
资产	存活IP	端口	软件	硬件	漏洞

1.2 任务详情

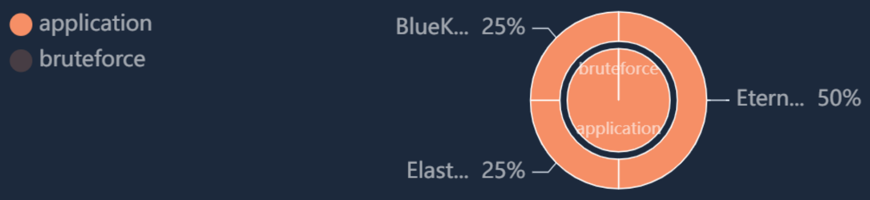
任务名称	
IP/Domain	172.16.13.0/24
端口	21,22,23,25,53,U:53,U:69,80,81,U:88,110,111,U:111,123,U:123,135,U:137,139,U:161,U:177,389,U:427,443,445,465,500,515,U:520,U:523,548,623,U:626,636,873,902,1080,1099,1433,U:1434,1521,U:1604,U:1645,U:1701,1883,U:1900,2049,2181,2375,2379,U:2425,3128,3306,3389,4730,U:5060,5222,U:5351,U:5353,5432,5555,5601,5672,U:5683,5900,5938,5984,6000,6379,7001,7077,8080,8081,8443,8545,8686,9000,9001,9042,9092,9200,9418,9999,11211,U:11211,27017,U:33848,37777,50000,50070,61616
漏洞	通用PoC
进度	100%
服务器	127.0.0.1
开始时间	2024-09-13 12:40:26
结束时间	2024-09-13 12:44:45
Goby版本	2.9.7

1.3 风险分布

风险资产分布

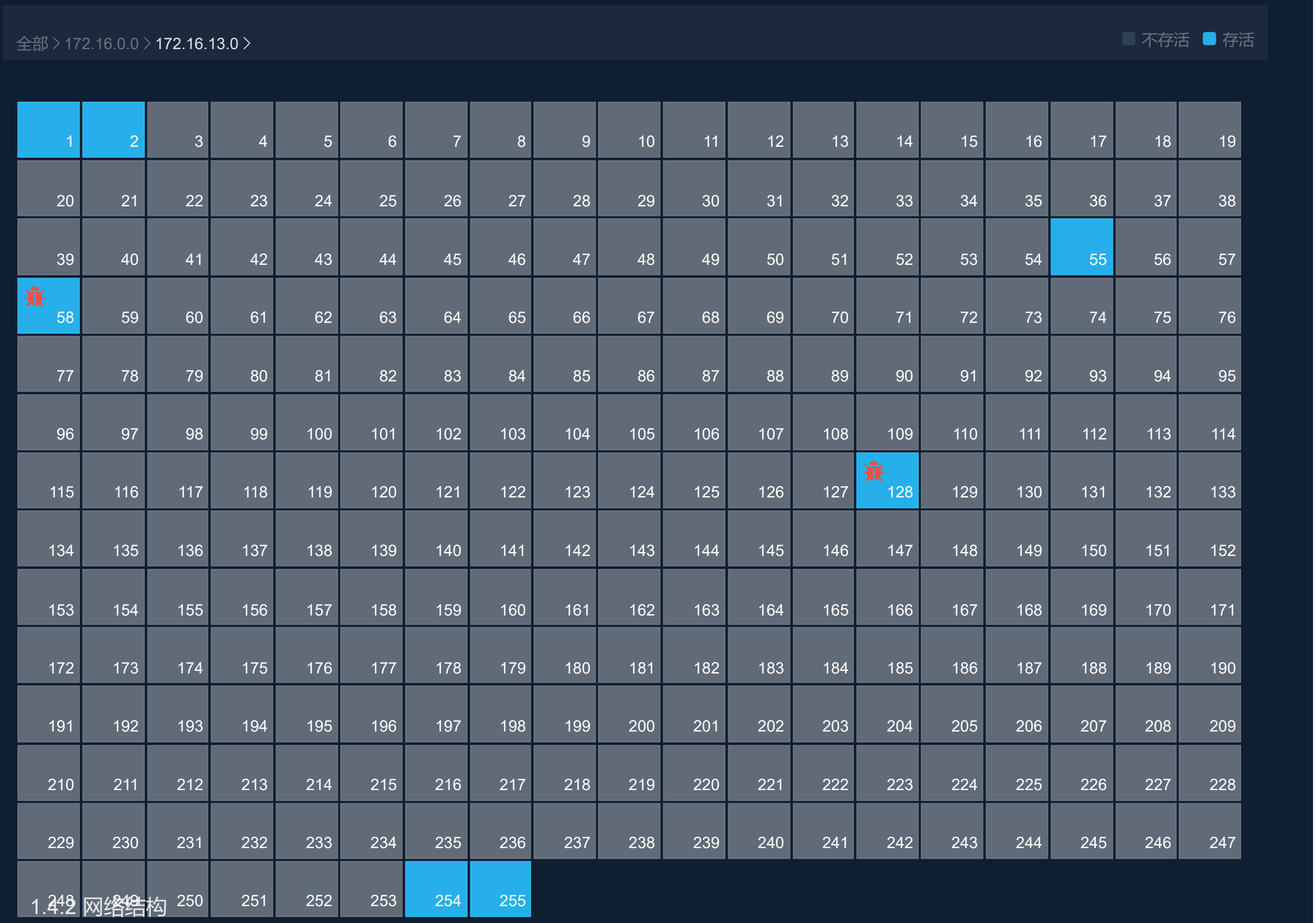


风险统计（TOP5)



1.4 资产分布

1.4.1 IP资源分布



全部 > 172.16.0.0 > 172.16.13.0 >

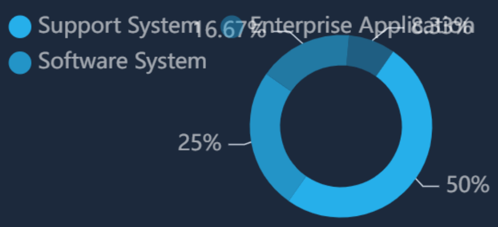
⬛ 不存活 🟦 存活

🟦 1	🟦 2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	🟦 55	56	57
🟦 🐞 58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76
77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114
115	116	117	118	119	120	121	122	123	124	125	126	127	🟦 🐞 128	129	130	131	132	133
134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152
153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171
172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209
210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228
229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247
248	249	250	251	252	253	🟦 254	🟦 255											

1.4.2 网络结构

暂无数据

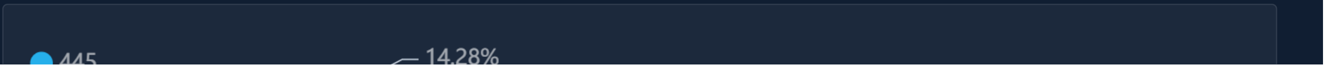
1.4.3 资产类型分布

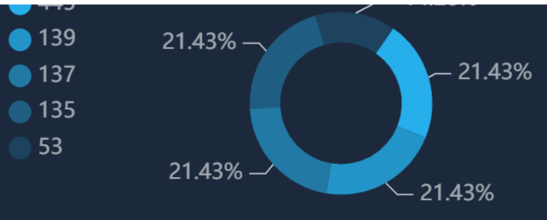


Support System	6	50.00%
Software System	3	25.00%
	2	16.67%
Enterprise Application	1	8.33%

共有：12

1.4.4 端口开放情况



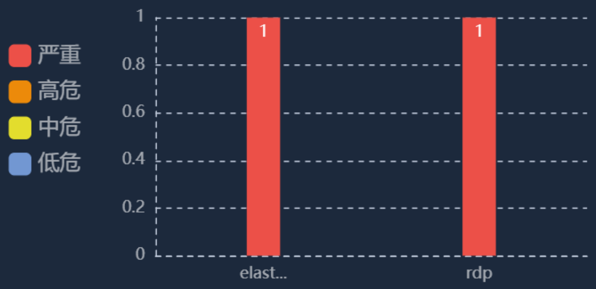


445	3	21.43%
139	3	21.43%
137	3	21.43%
135	3	21.43%
53	2	14.29%

共有：14

2. 风险分析

2.1 服务风险



服务	严重	高危	中危	低危	共有
elasti...	1	0	0	0	1
rdp	1	0	0	0	1

2.2 应用风险

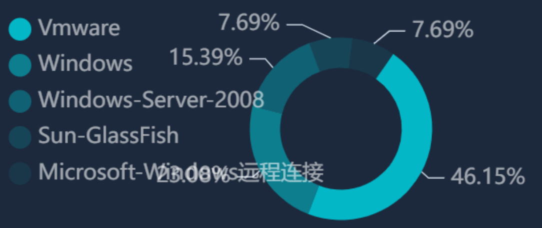
暂无数据

3. 资产分析

3.1 硬件

暂无数据

3.2 软件



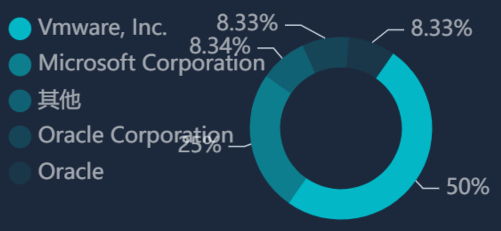
Vmware	6	46.15%
Windows	3	23.08%
Windows-Server-2008	2	15.38%
Sun-GlassFish	1	7.69%
Microsoft-Windows远程连接	1	7.69%

共有：13

3.3 硬件厂商

暂无数据

3.4 软件厂商



Vmware, Inc.	6	50.00%
Microsoft Corporation	3	25.00%
其他	1	8.33%
Oracle Corporation	1	8.33%
Oracle	1	8.33%
共有：12		

4. 漏洞

名称 (3)	等级	hostinfo	vulurl	keymemo
Eternalblue/DOUBLEPULSAR MS17-010 SMB RCE	严重	172.16.13.128:445	-	-
Eternalblue/DOUBLEPULSAR MS17-010 SMB RCE	严重	172.16.13.58:445	-	-
Elasticsearch unauthorized	严重	172.16.13.58:9200	http://172.16.13.58:9200/_cat	-
BlueKeep Microsoft Remote Desktop RCE (CVE-2019-0708)	严重	172.16.13.58:3389	-	-

BlueKeep Microsoft Remote Desktop RCE (CVE-2019-0708) 详情

严重 BlueKeep Microsoft Remote Desktop RCE (CVE-2019-0708)

漏洞摘要

风险类型	Other
披露时间	2019-05-14
URL	172.16.13.58:3389
参考	https://github.com/zerosum0x0/CVE-2019-0708/ https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708 http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Desktop-BlueKeep-Denial-Of-Service.html http://packetstormsecurity.com/files/153627/Microsoft-Windows-RDP-BlueKeep-Denial-Of-Service.html http://packetstormsecurity.com/files/154579/BlueKeep-RDP-Remote-Windows-Kernel-Use-After-Free.html http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-windows-en http://www.huawei.com/en/psirt/security-notices/huawei-sn-20190515-01-windows-en

	https://cert-portal.siemens.com/productcert/pdf/ssa-166360.pdf https://cert-portal.siemens.com/productcert/pdf/ssa-406175.pdf https://cert-portal.siemens.com/productcert/pdf/ssa-433987.pdf https://cert-portal.siemens.com/productcert/pdf/ssa-616199.pdf https://cert-portal.siemens.com/productcert/pdf/ssa-832947.pdf https://cert-portal.siemens.com/productcert/pdf/ssa-932041.pdf https://nvd.nist.gov/vuln/detail/CVE-2019-0708 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
标签	rce

描述

A remote code execution vulnerability exists in Remote Desktop Services - formerly known as Terminal Services - when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

漏洞危害

An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system

解决方案

Download patch from: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Elasticsearch unauthorized 详情

严重 Elasticsearch unauthorized

漏洞摘要

风险类型	Other
披露时间	2019-03-04
URL	http://172.16.13.58:9200/_cat
参考	https://fofa.info/
标签	unauthorized

描述

Elasticsearch is a Lucene-based search service. It provides a distributed full-text search engine that can serve multiple users based on RESTful web interfaces. Elasticsearch is developed in Java and open-source subject to the Apache license terms. It is the second most popular enterprise search engine.<br/>Designed for cloud computing, Elasticsearch features real-time search, stable, and reliable performance, fast response, and easy installation and usage. But unsafe use of Elasticsearch has also given rise to some problems. By default, after Elasticsearch is installed, the data information can be accessed and viewed in web announcements by using Port 9200.

漏洞危害

Elasticsearch's HTTP connections do not implement any permission control measures. Once deployed on a public network, Elasticsearch is prone to data leaks.

解决方案

- We recommend that you do not publish Elasticsearch's Port 9200 service on the Internet.<br/> - add auth

Eternalblue/DOUBLEPULSAR MS17-010 SMB RCE 详情

严重 Eternalblue/DOUBLEPULSAR MS17-010 SMB RCE

漏洞摘要

风险类型	Other
披露时间	2017-03-14
URL	172.16.13.128:445 172.16.13.58:445
参考	https://github.com/rapid7/metasploit-framework/blob/master//modules/exploits/windows/smb/ms17_010_eternalblue.rb https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010 https://zerosum0x0.blogspot.com/2017/04/doublepulsar-initial-smb-backdoor-ring.html
标签	rce

描述

Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server.

漏洞危害

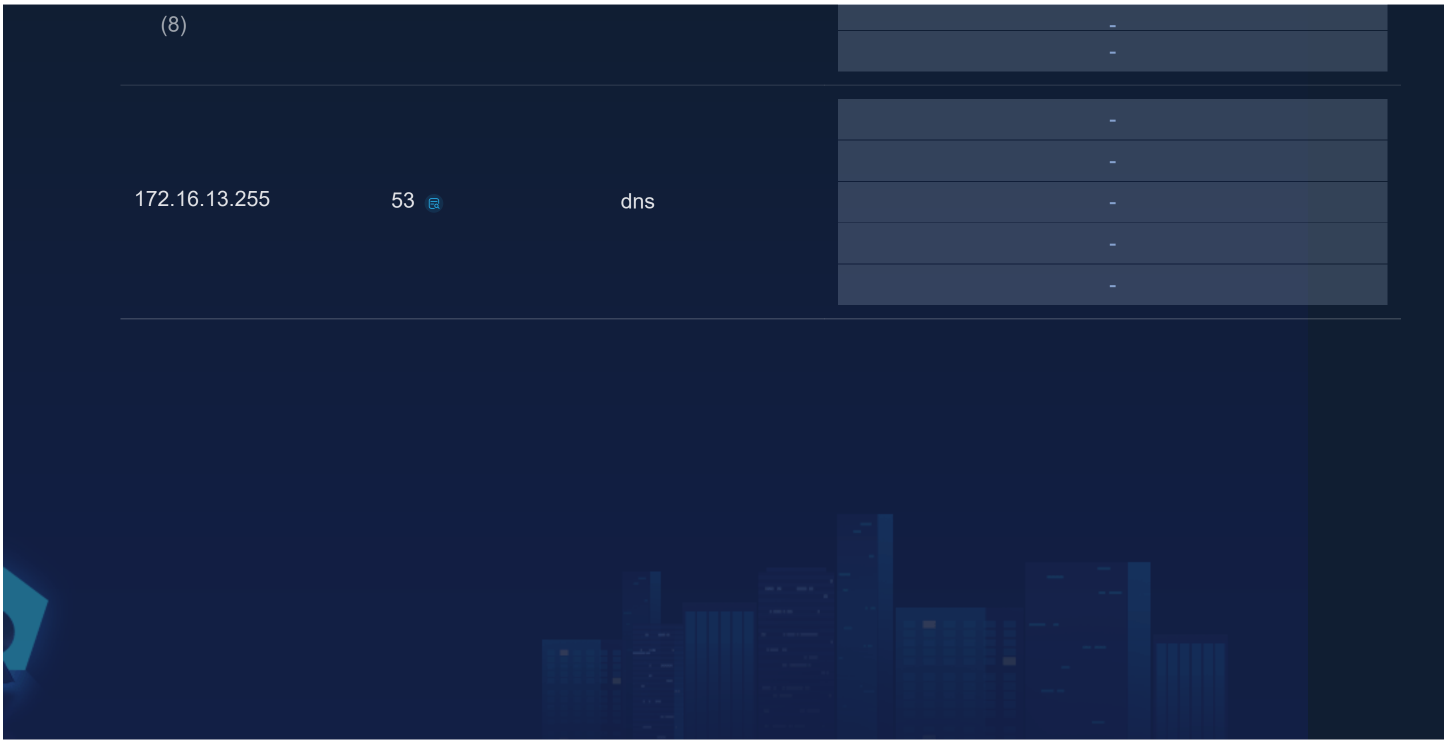
The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.

解决方案

Download patch from: https://support.microsoft.com/kb/4013389

5. 资产

IP	端口	协议	组件
172.16.13.58 ⚠ METASPL…	445 3389 139 137 8080 5iS… 80 wf… 21 9200 135	smb rdp netbios-ssn netbios http http ftp elastic dcerpc	rdp windows-smb ASP ASP.NET Java 25.112-b15 Log4j2 Microsoft-FTP Microsoft-Windows远程连接 IIS 7.5 Elasticsearch 1.1.1 Sun-GlassFish Windows 6.1.7601 Ntlm 15 Windows-Server-2008 Vmware
172.16.13.128 ⚠ W2K8 ,W2K8	445 139 137 135	smb netbios-ssn netbios dcerpc	windows-smb - - Windows 6.1.7601 Ntlm 15 Windows-Server-2008 Vmware
172.16.13.1 DESKTOP-…	445 139 137 135 5353	smb netbios-ssn netbios dcerpc unknown	- - - Windows 10.0.22621 Ntlm 15 Vmware
172.16.13.2	53	dns	- - - - Vmware
172.16.13.254	-	-	- - - - Vmware
172.16.13.55	-	-	- - - - Vmware
172.16.13.0	53	unknown	- - -



(8)			- -
172.16.13.255	53	dns	- - - - -