

2023 年

网络空间安全漏洞态势

分析研究报告

天融信阿尔法实验室

ALPHA LAB

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信阿尔法实验室

天融信科技集团

2024年1月

2023

2.1

2.2

2.3

2.4

2.5

2.6

2.7

0/

00



23900

2023

18635

22.03%

5.85%

46.93%

47.22%

2023

, 2023

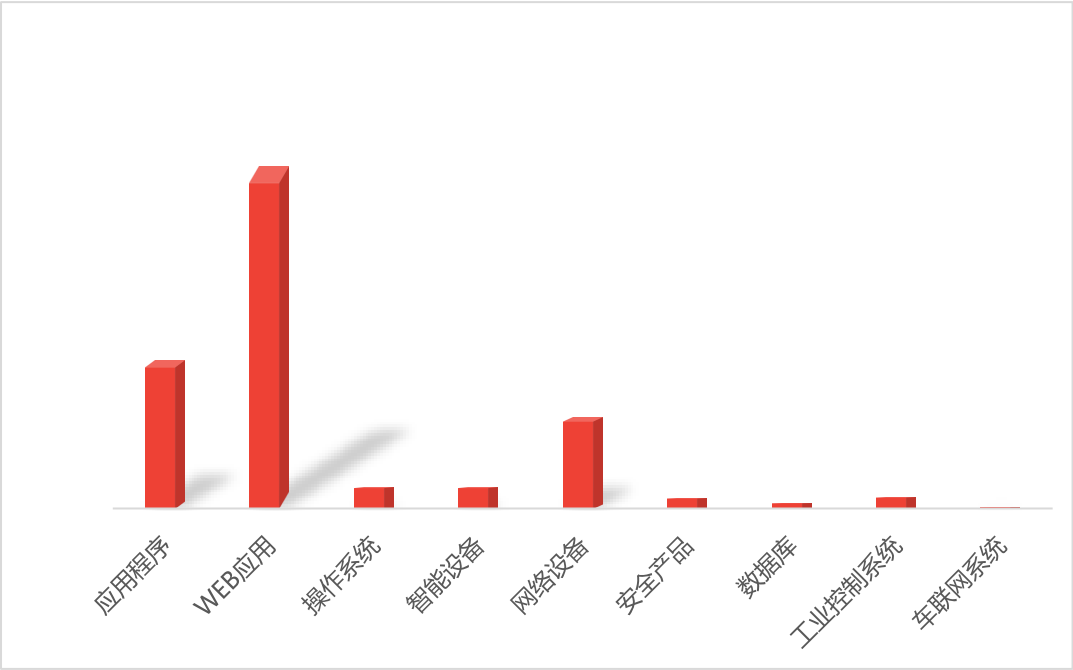
2023

1

(

CMD)

2.1



3 2023

(

QND)

2.3

2023

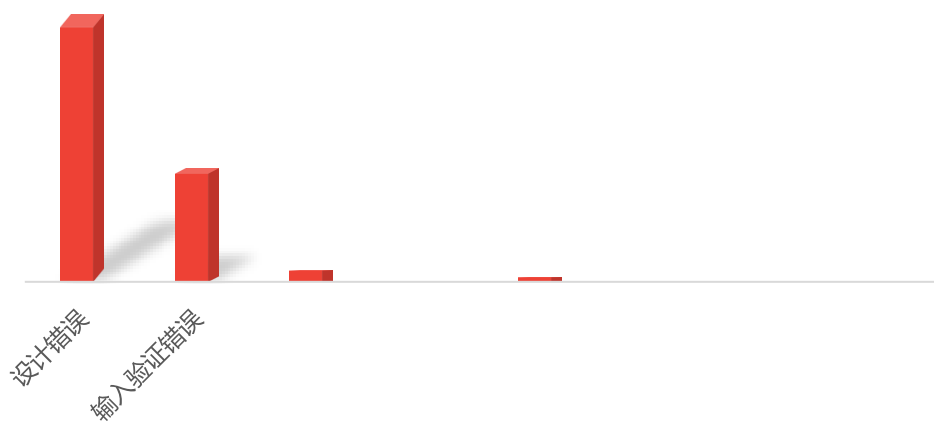
1-12

67.6%

28.5%

2.8%

0.9% 0.2% 0.1% 0.01% 0.004% 0.004%



4 2023

CMD

2.4

2023

1-12

27.7%

10.0%

54.9%

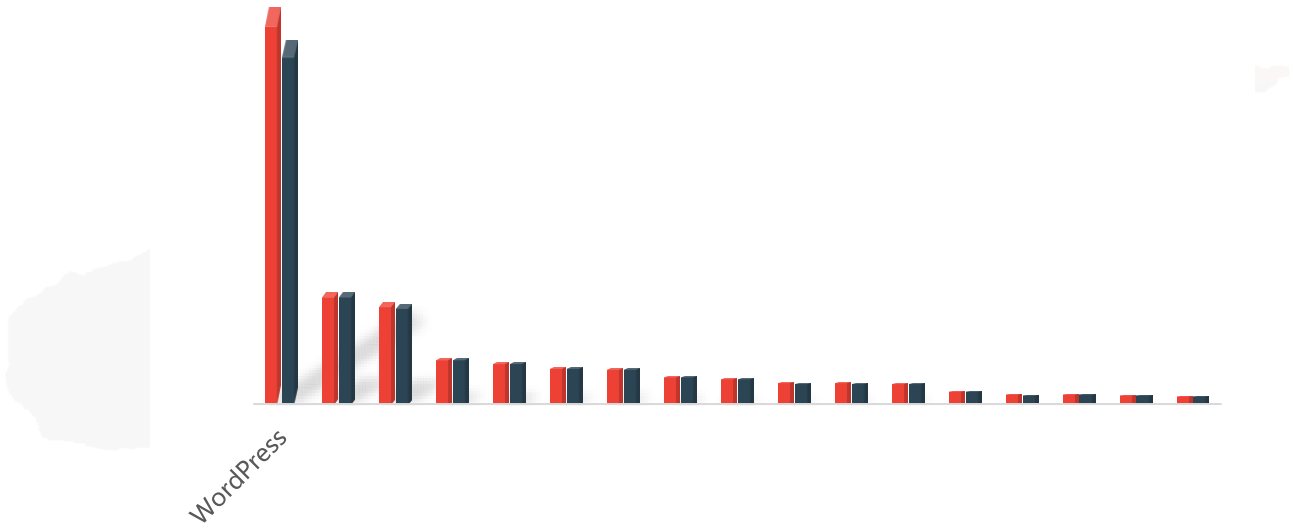
7.1% 0.2% 0.1%



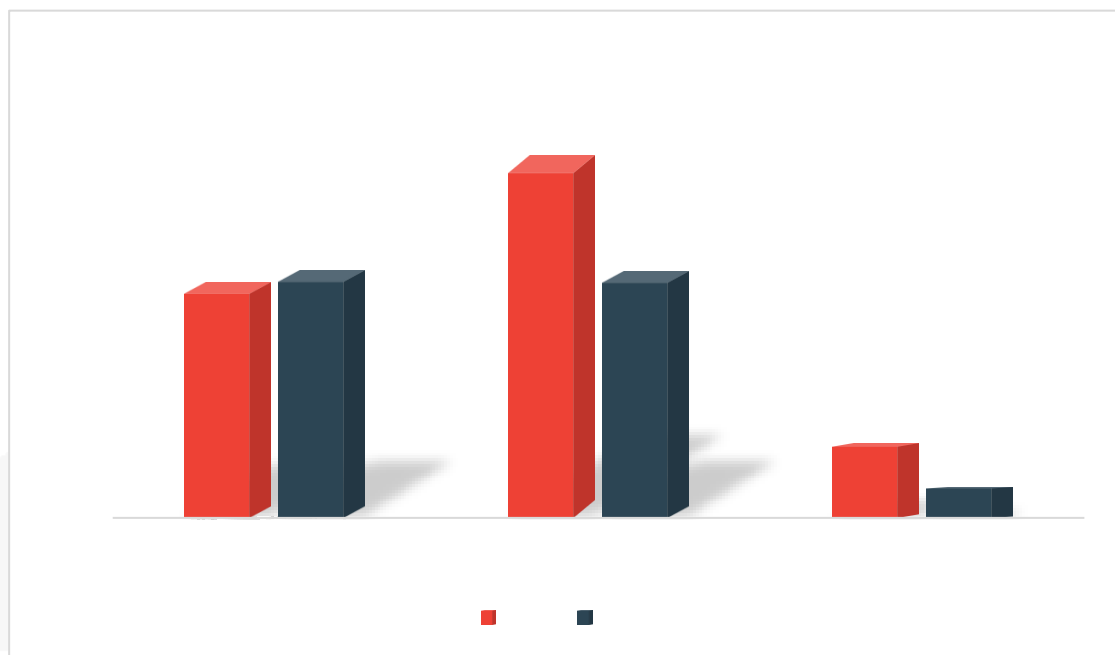
CWD

6 2023

QMD



Appl e	IBM	100%	7	2023	CNMD	Or acl e
2.7						
CNMD	2022	2023	2022	23900		
2023	18635	22.03%	2022	8379	2023	
8800	2022	5.02%	2022	12862	2023	
8745	2022	32.01%	2022	2659	2023	1090
2022	59.01%					



8 2023

QMD

2022

2023

2023

100

EXP

4

Microsoft

Google

Apple

:

3.1

Microsoft

Juniper Networks Apache Foundation Cisco

3.4

2023

100

31%

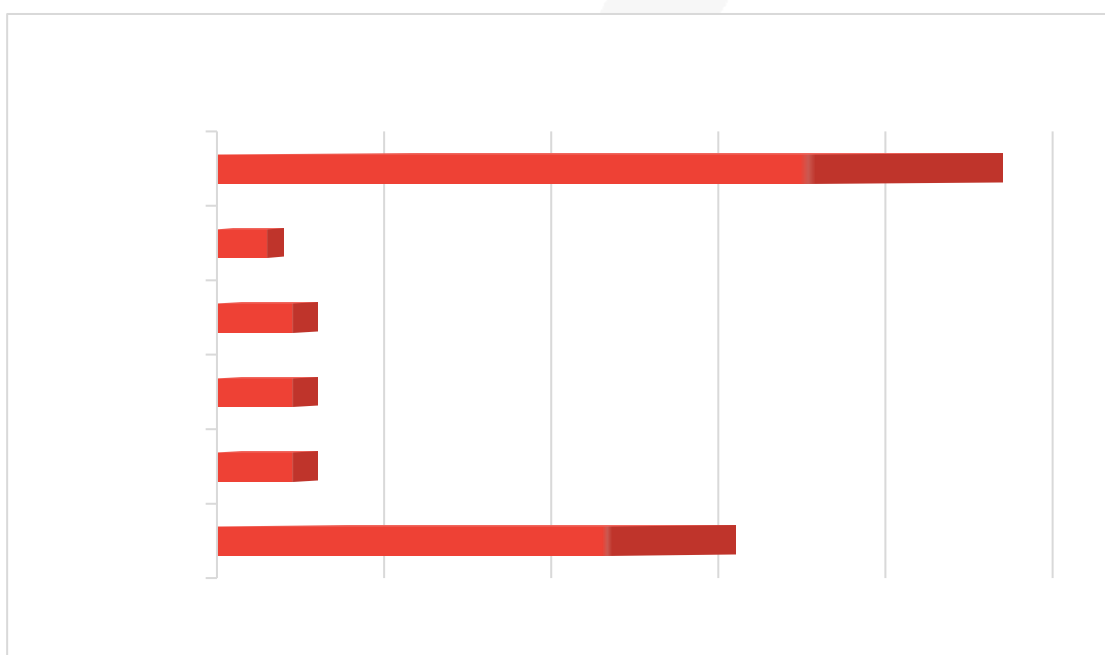
6%

6%

6%

4%

47%



10 TOP100

(

cyber security-help)

2023

47%

31%

3.5

2023

11 TOP100

(cyber secur i t y- hel p)

2023

MITRE

43996

CVE TOP 25

	ID			2022
1	CVE-787		63.72	0
2	CVE-79		45.54	0
3	CVE-89	SQL		

18	CVE-798		4.57	-3
19	CVE-918	(SSRF)	4.56	2
20	CVE-306		3.78	-2
21	CVE-362		3.53	1
22	CVE-269		3.31	7
23	CVE-94		3.3	2
24	CVE-863		3.16	4
25	CVE-276		3.16	-5

1 CVE TOP 25 (M TRE)

CVE 25

25

1	CVE-416	Use-After-Free	7	4
2	CVE-862		16	11
3	CVE-269		29	22
4	CVE-863		28	24
1	CVE-502		12	15
2	CVE-798		15	18
3	CVE-276		20	25
Top 25				
1	CVE-269		29	22
2	CVE-863		28	24

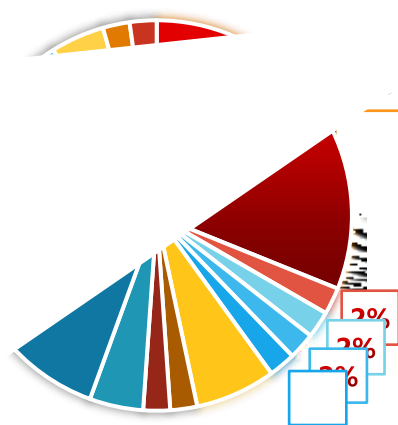
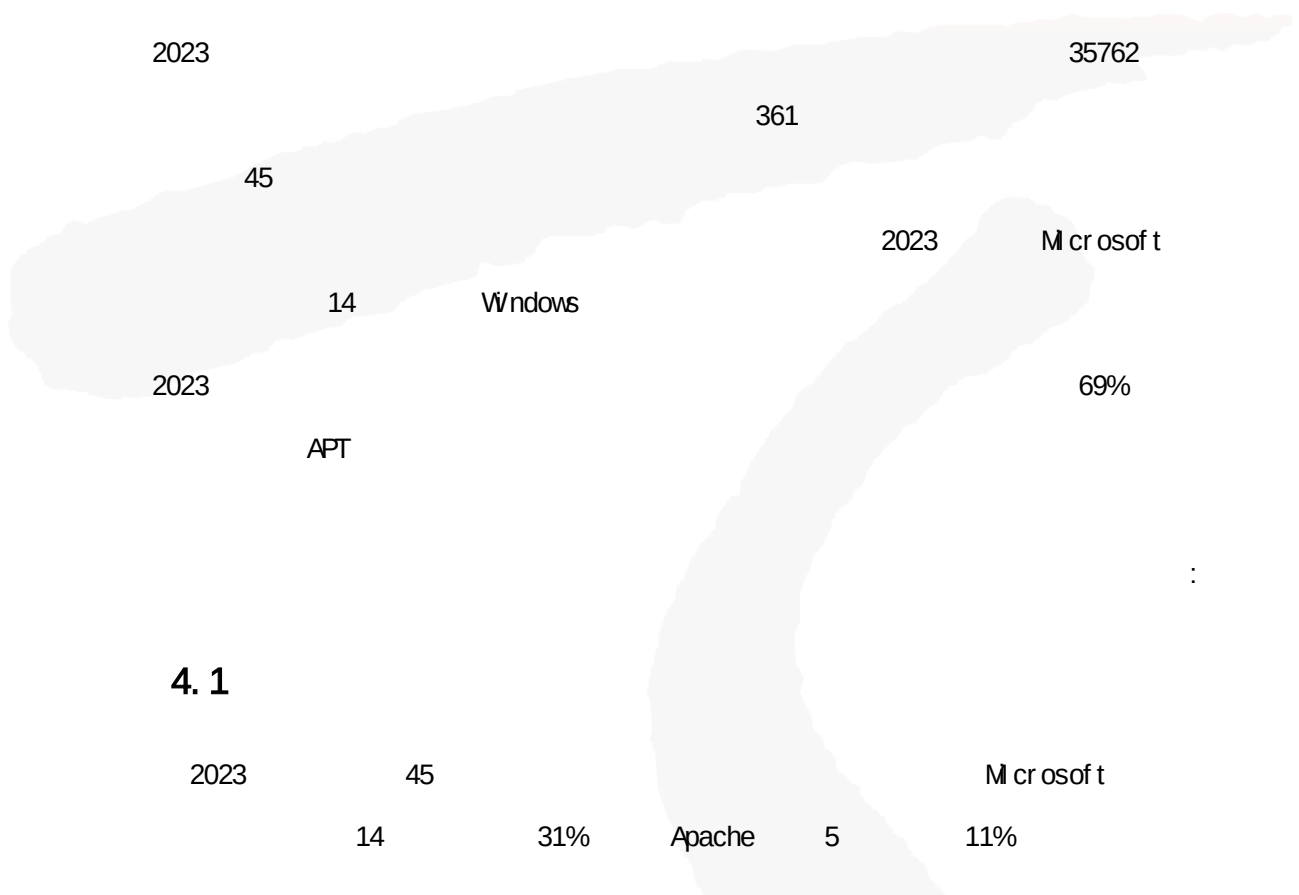
Top 25

1	CVE-400	23	37
2	CVE-611 XML	24	28

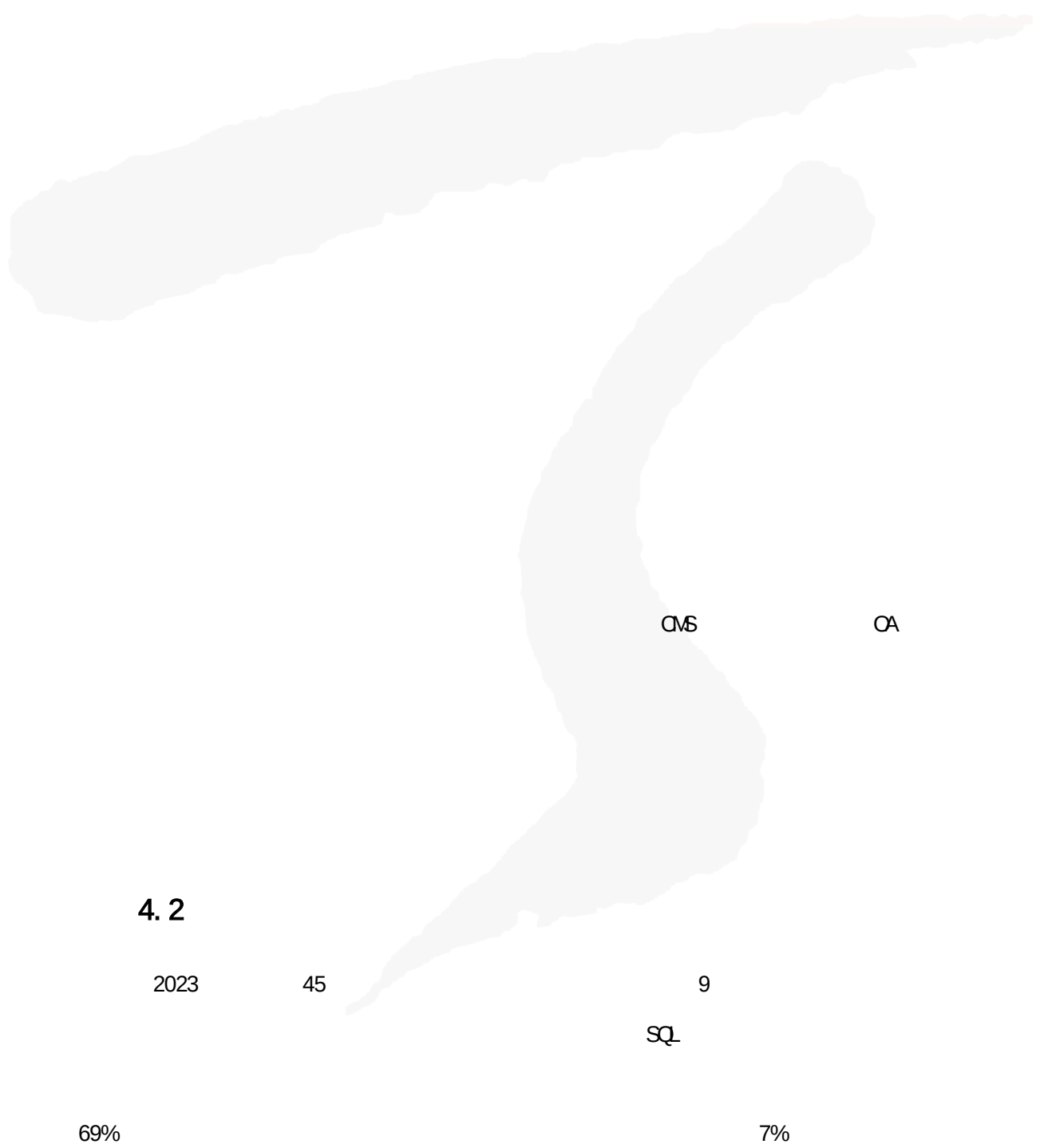
3.6 EXP

2023 100 EXP EXP
55% EXP 45%

12 TOP100



13 2023





14 2023

WebShell I ,

SQL

SQL

4.3 TOP10

2023

NO 1	CVE- 2023- 21716	Microsoft Word	CVE- 2023- 21716 RTF
NO 2	CVE- 2023- 33246	Apache Rocket MQ	CVE- 2023- 33246 Rocket MQ NameServer Broker Controller Rocket MQ
NO 3	CVE- 2023- 22518	Atlassian Confluence	CVE- 2023- 22518 Confluence Struts2
NO 4	CVE- 2023- 3269	Linux Kernel	CVE- 2023- 3269 Linux ROOT
NO 5	CVE- 2023- 3519	Citrix ADC Citrix Gateway	Citrix ADC Citrix Gateway VPN ICA VPN RDP AAA
NO 6	CVE- 2022- 41678	Apache ActiveMQ Jolokia	/api/jolokia/ MBean
NO 7	CVE- 2023- 50164	Apache Struts2	CVE- 2023- 50164

NO 8	CVE- 2023- 38646	Met abase	CVE- 2023- 38646 Met abase H2 H2 JDBC Met abase
NO 9	CVE- 2023- 20860	Spring Framework	Spring Framework Spring Security Spring Security Spring MVC mvcRequest Mat cher
NO 10	CVE- 2023- 37582	Apache Rocket MQ	CVE- 2023- 37582 33246 NameSer ver Rocket MQ Rocket MQ

2 TOP10

4.4 TOP10

Microsoft Word
CVE- 2023- 21716 CVSS 3. 1/ AV: N AC L/ PR N U: N S U C H I: H A: H 9. 8 2023- 4- 7 CVE- 2023- 21716 Microsoft Word RTF wwI b RTF

RTF

Windows

Microsoft Outlook

Apache Rocket MQ

CVE-2023-33246

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

9.8

2023-6-5

Rocket MQ 5.1.0

Rocket MQ NameServer Broker Controller

Rocket MQ

Rocket MQ

Rocket MQ 5.x

5.1.1

Rocket MQ 4.x

4.9.6

Atlassian Confluence

CVE-2022-22965

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

9.8

Conf l uence Dat a Cent er 60(x 5, €

per x̃, ε

CVE-2023-3519

CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

9.8

2023-7-27

Citrix ADC

Citrix Gateway

Citrix ADC

SSL/TLS

CVE-2023-3519

Citrix ADC

Citrix Gateway

VPN

ICA

VPN RDP

AAA

Apache Act i veMQ Jol oki a

CVE-2022-41678

CVSS 3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

8.8

2023-11-30

Jol oki a

Act i veMQ

j et t y

or g. j ol oki a. ht t p. Agent Ser vl et

/ api / j ol oki a

or g. j ol oki a. ht t p. H t t pRequest Handl er #handl ePost Request

JSONObj ect

JmxRequest

or g. j ol oki a. ht t p. H t t pRequest Handl er #execut eRequest

org.jolokia.handler.ExecHandler#doHandleRequest

Java 11 jdk.management.jfr.FlightRecorderMXBeanImpl RCE 1

newRecording 2 setConfiguration webshell 3

4 copyTo Webshell.jsp

Jolokia Jolokia Acti veMQ

Jolokia Acti veMQ Jolokia

5.16.6 5.17.4 5.18.0 6.0.0

Apache Struts2

CVE-2023-50164

CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

9.8

2023-12-11

Apache Struts

2017

Equifax

Equifax

1.45

7

Equifax

200,000

Apache Software Foundation

Struts 2

CVE-2023-50164

Struts 2.5.33

Struts 6.3.0.2

Metabase

CVE-2023-37470

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

9.8

2023-7-27

Metabase

CSV

0.46.6.1

Metabase

1.46.6.1

Metabase Enterprise

Spring Framework

CVE-2023-20860

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

7.5

2023-4-7

Spring Framework

Java

JDBC

Hibernate

Spring

Spring MVC

Spring Security

Spring

Data Spring Batch

Spring Framework

Java

6.0.0 - 6.0.6

5.3.0 - 5.3.25

Spring Framework

mvcRequestMatcher

Spring

Security

Spring Security

Spring MVC

Apache Rocket MQ

CVE- 2023- 37582

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

9.8

2023- 7- 18

Apache Rocket MQ

Rocket MQ

/

Rocket MQ

Rocket MQ NameSer ver

CVE- 2023- 33246

5. 1. 1

NameSer ver

NameSer ver

Rocket MQ

NameSer ver

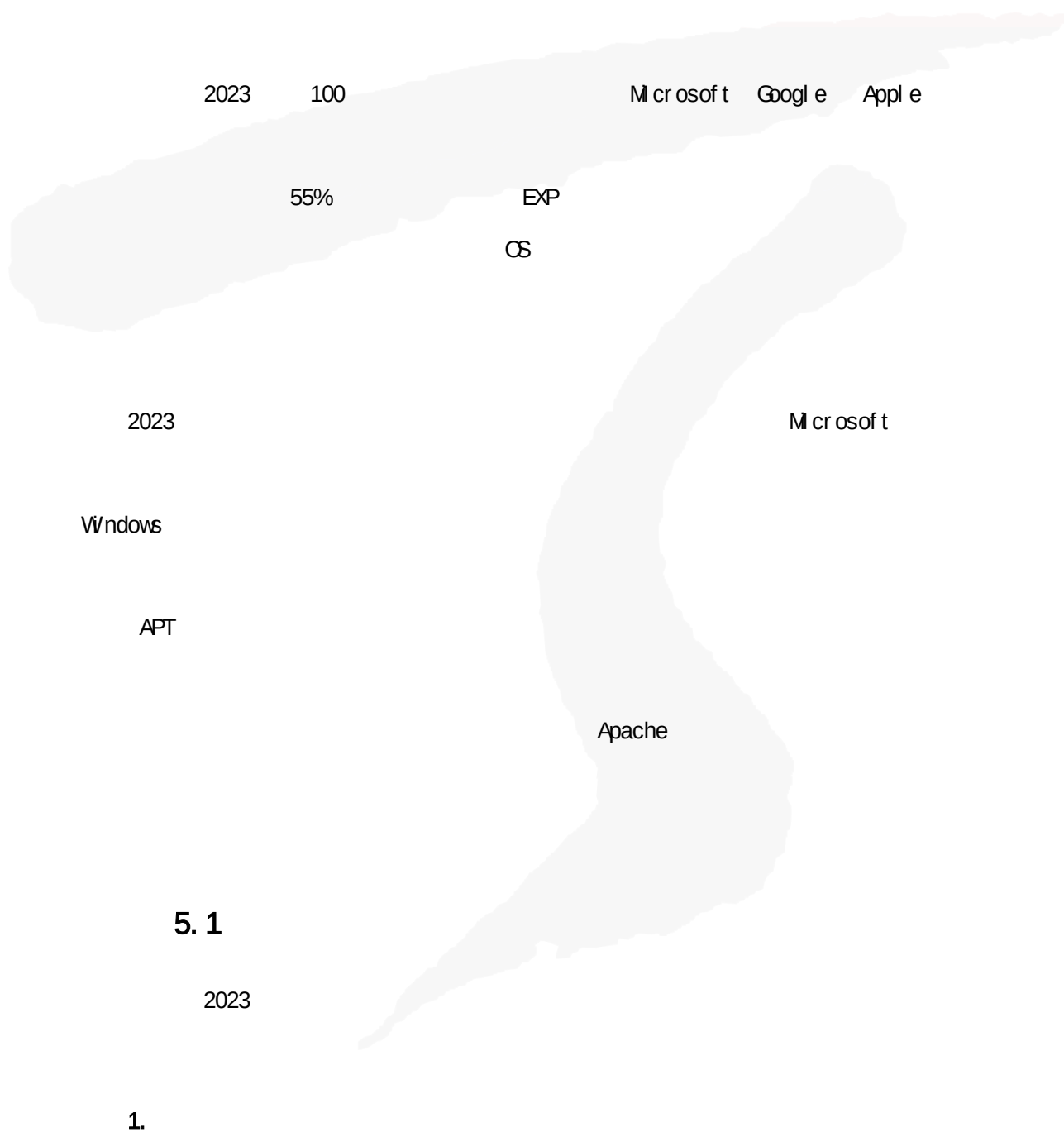
Rocket MQ 5. x

5. 1. 2

Rocket MQ 4. x

NameSer ver

4. 9. 7

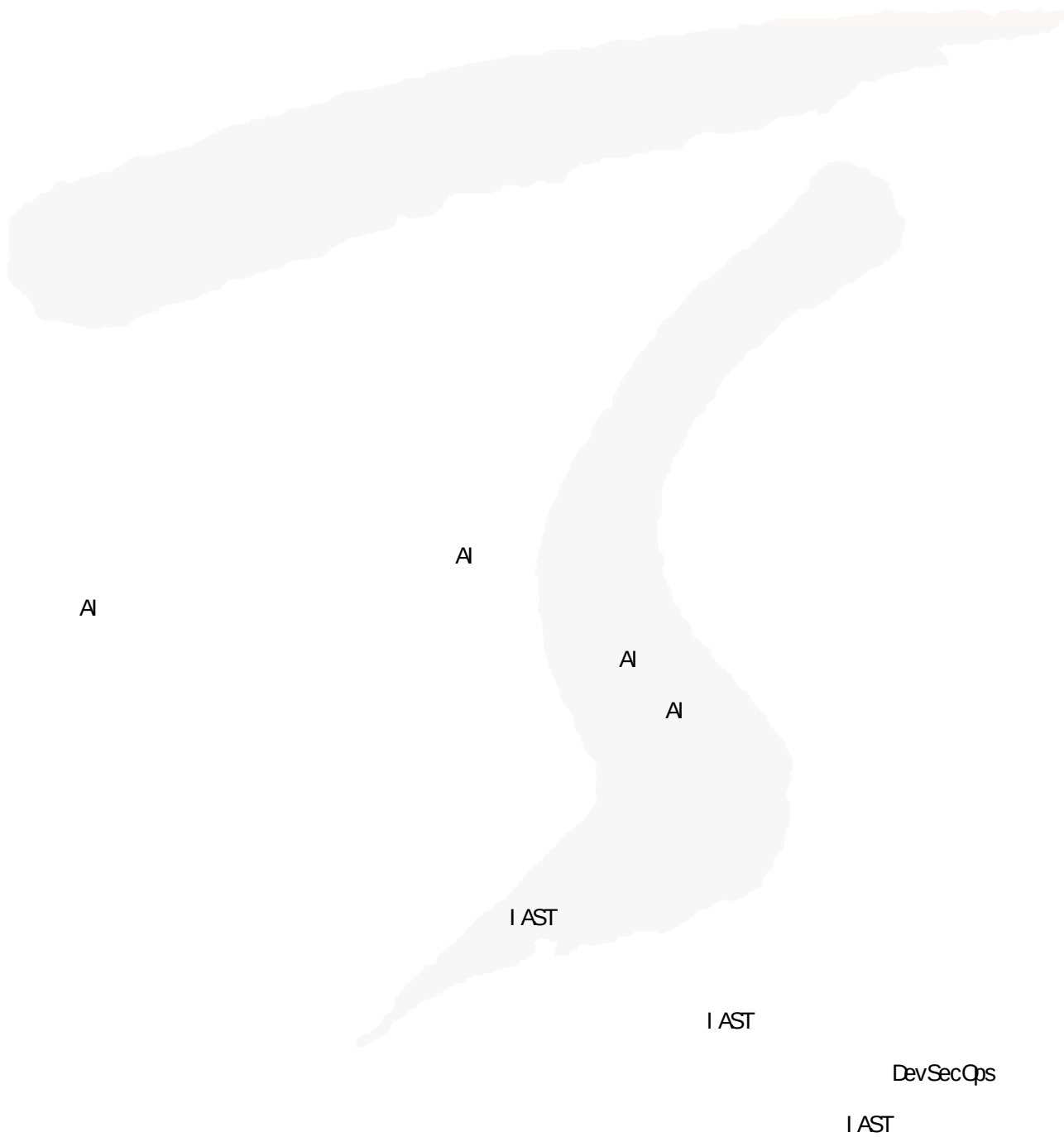


2.

3.

4.

2024



7 24

IT