

北京师范大学网络信息安全通告

2022 年 2 月报告

北京师范大学信息网络中心

2022 年 3 月

目录

漏洞态势	2
1. 公开漏洞情况.....	2
1.1. 漏洞增长概况.....	2
1.2. 漏洞分布情况.....	3
1.2.1. 漏洞厂商分布	3
1.2.2. 漏洞产品分布	3
1.2.3. 漏洞类型分布	4
1.2.4. 漏洞危害等级分布	5
1.3. 漏洞修复情况.....	5
1.3.1. 整体修复情况	5
1.3.2. 厂商修复情况	6
1.4. 重要漏洞实例.....	7
1.4.1. 超危漏洞实例	7
1.4.2. 高危漏洞实例	14
2. 漏洞平台推送情况.....	26
3. 接报漏洞情况.....	26
4. 重大漏洞预警.....	28
4.1. Fortinet FortiWeb安全漏洞的预警.....	28
4.2. 微软多个安全漏洞的预警.....	29

漏洞态势

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2022年2月份新增安全漏洞共1859个，从厂商分布来看，WordPress基金会公司产品的漏洞数量最多，共发布165个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到12.91%。本月新增漏洞中，超危漏洞272个、高危漏洞698个、中危漏洞850个、低危漏洞39个，相应修复率分别为80.88%、89.68%、92.35%以及94.87%。合计1668个漏洞已有修复补丁发布，本月整体修复率89.73%。

截至2022年2月28日，CNNVD采集漏洞总量已达178577个。

1.1 漏洞增长概况

2022年2月新增安全漏洞1859个，与上月（2054个）相比减少了9.49%。根据近6个月来漏洞新增数量统计图，平均每月漏洞数量达到1835个。

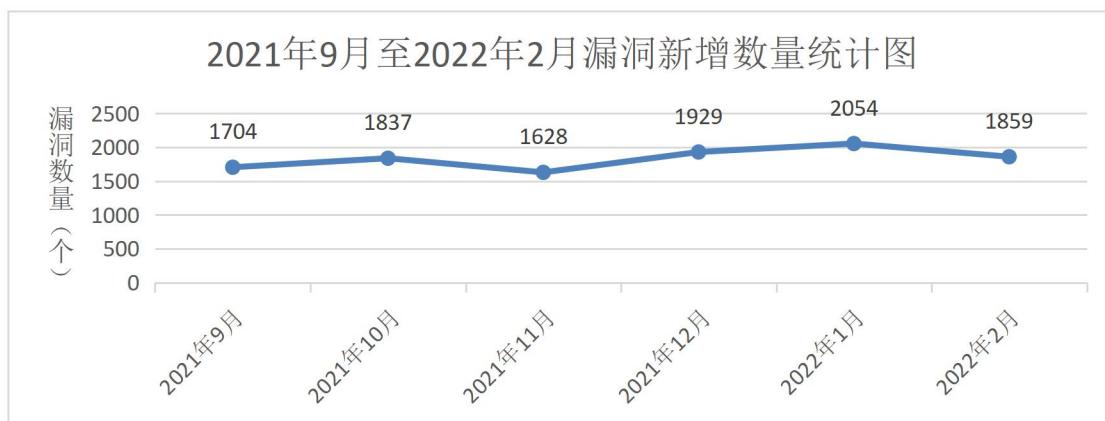


图1 2021年9月至2022年2月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2022年2月厂商漏洞数量分布情况如表1所示，WordPress基金会公司漏洞达到165个，占本月漏洞总量的8.88%。

表1 2022年2月排名前十厂商新增安全漏洞统计表

序号	厂商名称	漏洞数量(个)	所占比例
1	WordPress 基金会	165	8.88%
2	Google	125	6.72%
3	Intel	75	4.03%
4	Tenda	55	2.96%
5	Microsoft	51	2.74%
6	Git	30	1.61%
7	JetBrains	29	1.56%
8	Siemens	27	1.45%
9	D-Link	26	1.40%
10	Cisco	25	1.34%

1.2.2 漏洞产品分布

2022年2月主流操作系统的漏洞统计情况如表2所示。本月Windows系列操作系统漏洞数量共26个，Android漏洞数量最多，共25个，占主流操作系统漏洞总量的11.85%，排名第一。

表2 2022年2月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	Android	25
2	Windows 11	22
3	Windows 10	21
4	Windows Server 2022	21

5	Windows Server 2019	20
6	Windows Server 2016	16
7	Windows Server 2012	13
8	Windows Server 2012 R2	13
9	Windows 8.1	13
10	Windows Rt 8.1	13
11	Windows 7	10
12	Windows Server 2008	10
13	Windows Server 2008 R2	10
14	Linux Kernel	4

1.2.3 漏洞类型分布

2022年2月份发布的漏洞类型分布如表3所示，其中缓冲区错误类漏洞所占比例最大，约为12.91%。

表3 2022年2月漏洞类型统计表

序号	漏洞类型	漏洞数量(个)	所占比例
1	缓冲区错误	240	12.91%
2	跨站脚本	210	11.30%
3	输入验证错误	123	6.62%
4	代码问题	111	5.97%
5	资源管理错误	84	4.52%
6	SQL注入	74	3.98%
7	访问控制错误	63	3.39%
8	信息泄露	60	3.23%
9	命令注入	54	2.90%
10	跨站请求伪造	52	2.80%
11	授权问题	45	2.42%
12	权限许可和访问控制问题	43	2.31%
13	代码注入	41	2.21%
14	路径遍历	40	2.15%
15	信任管理问题	26	1.40%
16	操作系统命令注入	24	1.29%
17	安全特征问题	12	0.65%
18	注入	11	0.59%
19	竞争条件问题	8	0.43%
20	后置链接	8	0.43%
21	加密问题	6	0.32%

22	数字错误	6	0.32%
23	日志信息泄露	4	0.22%
24	环境问题	4	0.22%
25	数据伪造问题	4	0.22%
26	格式化字符串错误	1	0.05%
27	默认配置问题	1	0.05%
28	其他	504	27.11%

1.2.4 漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即超危、高危、中危和低危级别。2022年2月漏洞危害等级分布如图2所示，其中超危漏洞272条，占本月漏洞总数的14.63%。

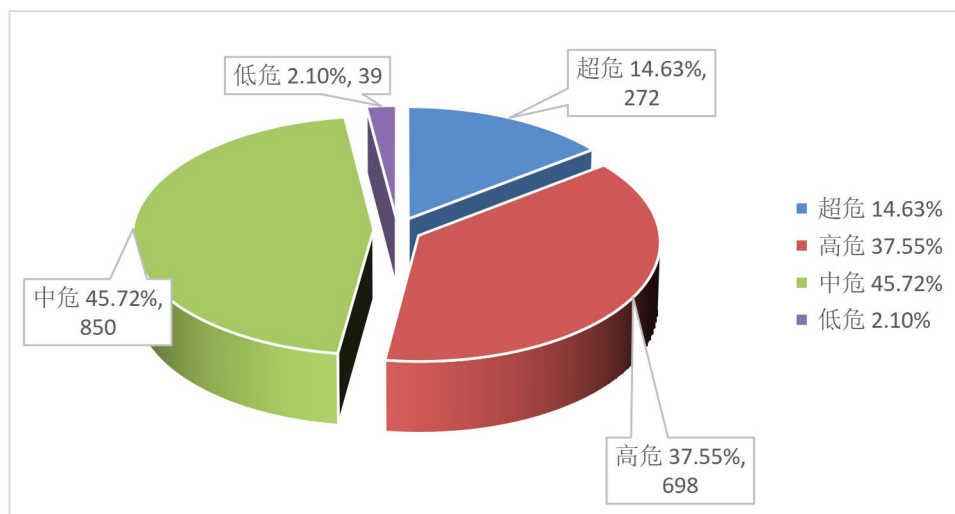


图2 2022年2月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

2022年2月漏洞修复情况按危害等级进行统计见图3。其中低危漏洞修复率最高，达到94.87%，超危漏洞修复率最低，比例为80.88%。

总体来看，本月整体修复率，由上月的 83.89% 上升至本月的 89.73%。

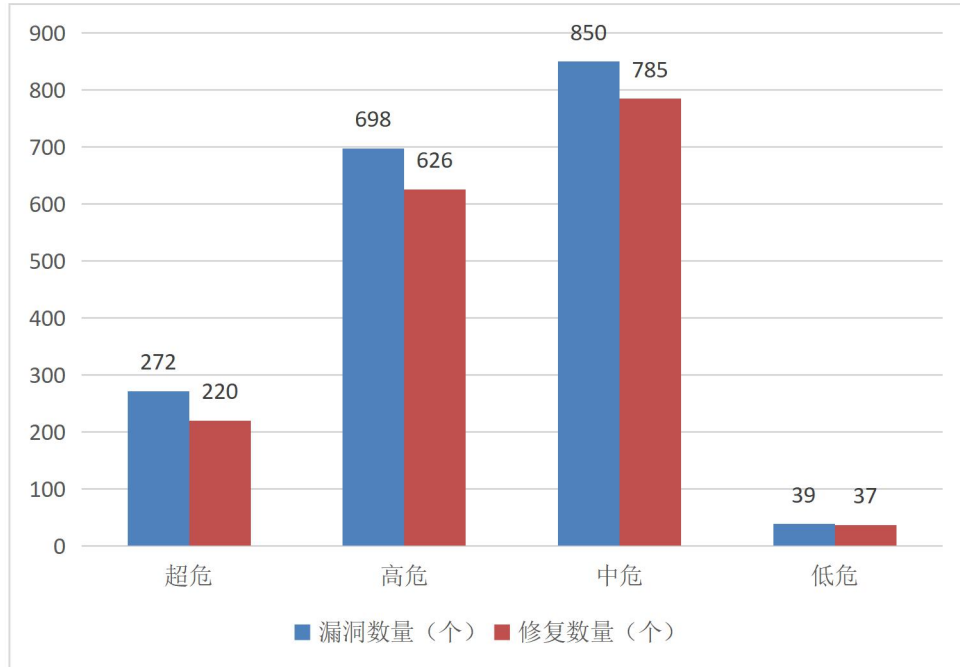


图 3 2022 年 2 月漏洞修复数量统计

1.3.2 厂商修复情况

2022 年 2 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 WordPress 基金会、Google、Intel 等十个厂商共 608 条漏洞，占本月漏洞总数的 32.71%，漏洞修复率为 90.13%，详细情况见表 4。多数知名厂商对产品安全高度重视，产品漏洞修复比较及时，其中 Intel、Microsoft、Git、JetBrains、Siemens、Cisco 等公司本月漏洞修复率均为 100%，共 548 条漏洞已全部修复。

表 4 2022 年 2 月厂商修复情况统计表

序号	厂商名称	漏洞数量 (个)	修复数量	修复率
1	WordPress 基金会	165	162	98.18%
2	Google	125	123	98.40%
3	Intel	75	75	100.00%
4	Tenda	55	3	5.45%

5	Microsoft	51	51	100.00%
6	Git	30	30	100.00%
7	JetBrains	29	29	100.00%
8	Siemens	27	27	100.00%
9	D-Link	26	23	88.46%
10	Cisco	25	25	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

2022年2月超危漏洞共272个，其中重要漏洞实例如表5所示。

表5 2022年2月超危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例	
SQL注入	Desdev	CNNVD-202202-1166	WordPress 插件Paid Memberships Pro SQL注入漏洞 (CNNVD-202202-536)	
	EasyCMS社区	CNNVD-202202-1324		
	Elite Graphix			CNNVD-202202-066
				CNNVD-202202-067
				CNNVD-202202-069
				CNNVD-202202-071
				CNNVD-202202-072
	JeecgBoot社区			CNNVD-202202-1364
				CNNVD-202202-1370
	Lansweeper			CNNVD-202202-2166
				CNNVD-202202-2193
	Metinfo			CNNVD-202202-1169
				CNNVD-202202-1170
	MingSoft	CNNVD-202202-1404		
	S-CMS	CNNVD-202202-1171		
	Sourcecodester			CNNVD-202202-090
				CNNVD-202202-091
	Synology			CNNVD-202202-507
				CNNVD-202202-509
				CNNVD-202202-510
TSG	CNNVD-202202-958			
Tongda		CNNVD-202202-1179		
		CNNVD-202202-1181		
VoIPmonitor团队	CNNVD-202202-315			
WordPress基金会	CNNVD-202202-043			

		CNNVD-202202-536		
		CNNVD-202202-1892		
		CNNVD-202202-1894		
	个人开发者	CNNVD-202202-389		
		CNNVD-202202-1359		
		CNNVD-202202-1578		
		CNNVD-202202-1627		
代码问题	Airspan Networks	CNNVD-202202-204	PrinterLogic Web Stack 代码问题漏洞 (CNNVD-202202-142)	
	Celartem	CNNVD-202202-1777		
	Foxit	CNNVD-202202-1025		
	JqueryForm.com	CNNVD-202202-1375		
	MingSoft	CNNVD-202202-1607		
	PrinterLogic	CNNVD-202202-142		
	Qualcomm	CNNVD-202202-500		
	Red Hat	CNNVD-202202-1596		
	个人开发者			CNNVD-202202-723
				CNNVD-202202-956
		CNNVD-202202-970		
		CNNVD-202202-1024		
		CNNVD-202202-1174		
蓝智科技	CNNVD-202202-334			
授权问题	Airspan Networks	CNNVD-202202-207	Emerson Xweb-500 授权问题漏洞 (CNNVD-202202-1144)	
	Arista Networks	CNNVD-202202-354		
	Bmc Software	CNNVD-202202-953		
	Emerson	CNNVD-202202-1144		
	ForgeRock	CNNVD-202202-1187		
	Gitea社区	CNNVD-202202-836		
	Nokia	CNNVD-202202-1053		
	Northstar	CNNVD-202202-321		
	Qnap	CNNVD-202202-1023		
	Qualcomm	CNNVD-202202-503		
	Servisnet	CNNVD-202202-381		
	TIBCO	CNNVD-202202-1289		
	TP-Link	CNNVD-202202-1423		
个人开发者	CNNVD-202202-1143			
操作系统 命令注入	Airspan Networks	CNNVD-202202-196	Airspan Networks Mimosa Management Platform等产 品 操作系统命令注入漏洞 (CNNVD-202202-196)	
	D-Link			CNNVD-202202-241
				CNNVD-202202-242
				CNNVD-202202-243
				CNNVD-202202-1416
				CNNVD-202202-1417
Northstar	CNNVD-202202-318			

	Ricon Mobile	CNNVD-202202-093	
	Secuwiz	CNNVD-202202-911	
	个人开发者	CNNVD-202202-430	
缓冲区错误	Artifex Software	CNNVD-202202-1176	NGINX NGINX JavaScript模块 缓冲区错误漏洞 (CNNVD-202202-1182)
	Cisco	CNNVD-202202-120	
		CNNVD-202202-166	
		CNNVD-202202-168	
		CNNVD-202202-170	
		CNNVD-202202-173	
		CNNVD-202202-174	
		CNNVD-202202-175	
		CNNVD-202202-176	
	Facebook	CNNVD-202202-131	
	Foxit	CNNVD-202202-1028	
	Google	CNNVD-202202-476	
	Insyde	CNNVD-202202-103	
		CNNVD-202202-107	
	NGINX	CNNVD-202202-1182	
	Ricoh	CNNVD-202202-1296	
	Sealevel Systems	CNNVD-202202-096	
		CNNVD-202202-097	
	Sourceforge社区	CNNVD-202202-1591	
	TOTOLink	CNNVD-202202-254	
	Tenda	CNNVD-202202-1297	
CNNVD-202202-1299			
CNNVD-202202-1300			
CNNVD-202202-1301			
CNNVD-202202-1302			
Xerox	CNNVD-202202-1298		
个人开发者	CNNVD-202202-779		
	CNNVD-202202-1361		
	CNNVD-202202-1362		
	CNNVD-202202-1363		
	CNNVD-202202-1365		
	CNNVD-202202-1395		
CNNVD-202202-2155			
访问控制错误	Schneider Electric	CNNVD-202202-1051	Schneider Electric Interactive Graphical SCADA System Data Collector 访问控制错误漏洞 (CNNVD-202202-1051)
	个人开发者	CNNVD-202202-1675	
资源管理	NGINX	CNNVD-202202-1196	NGINX NGINX JavaScript模

错误	StarWind	CNNVD-202202-447	块 资源管理错误漏洞 (CNNVD-202202-1196)
	个人开发者	CNNVD-202202-727	
		CNNVD-202202-1323	
		CNNVD-202202-1757	
输入验证 错误	Accusoft	CNNVD-202202-1805	Schneider Electric Interactive Graphical SCADA System Data Server 输入验证错误漏洞 (CNNVD-202202-909)
	Adobe	CNNVD-202202-1106	
	Huawei	CNNVD-202202-860	
	Samsung	CNNVD-202202-1064	
	Schneider Electric	CNNVD-202202-909	
	TmaxSoft	CNNVD-202202-1585	
	个人开发者	CNNVD-202202-1316	
CNNVD-202202-1615			

1.WordPress 插件 Paid Memberships Pro SQL 注入 漏洞 (CNNVD-202202-536)

WordPress是WordPress基金会的一套使用PHP语言开发的博客平台。该平台支持在PHP和MySQL的服务器上架设个人博客网站。

WordPress插件Paid Memberships Pro存在SQL注入漏洞，该漏洞源于未对discount_code中的特殊字符安全处理。攻击者利用该漏洞可执行恶意SQL语句。以下版本受到影响：WordPress 插件 Paid Memberships Pro 2.6.7 之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://wpscan.com/vulnerability/6c25a5f0-a137-4ea5-9422-8ae393d7b76b>

2.PrinterLogic Web Stack代码问题漏洞 (CNNVD-202202-142)

PrinterLogic是美国PrinterLogic公司的一套企业打印管理软件。该软件用于无服务器远程站点打印机部署的企业打印机管理解决方案。

PrinterLogic组件Web Stack 19.1.1.13 存在安全漏洞，该漏洞源于

服务器未对接受的URL请求进行安全验证。攻击者利用该漏洞发送构造的URL会导致服务器端请求伪造。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.printerlogic.com/security-bulletin/>

3.Emerson Xweb-500 授权问题漏洞（CNNVD-202202-1144）

Emerson Xweb-500 是美国Emerson公司的一个基于Web服务器技术的数据记录和远程监控系统。

Emerson Xweb-500 存在安全漏洞，该漏洞源于Emerson Dixell XWEB-500 组件cgi-bin logo extra upload.cgi、cgi-bin cal save.cgi和cgi-bin lo utils.cgi缺少身份验证机制。未经身份验证的攻击者利用该漏洞可向目标系统写入任何文件，会导致拒绝服务或远程代码执行。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

<https://www.swascan.com/emerson>

4. Airspan Networks Mimosa Management Platform等产品操作系统命令注入漏洞（CNNVD-202202-196）

Airspan Networks Mimosa Management Platform（MMP）是美国Airspan Networks公司无线网络管理平台，MMP支持端到端网络管理等。

MMP存在操作系统命令注入漏洞，该漏洞源于软件对输入验证不当。未经身份验证的攻击者利用该漏洞可将专门制作的数据传递给应用程序，并在目标系统上执行任意命令。以下产品版本受到影响：

MMP 1.0.3 之前所有版本，PTP C系列 2.8.6.1 之前设备版本，PTMP C

系列及A5x 2.5.4.1 之前设备版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://cloud.mimosa.co/app/index.html#/updateFirmware/firmware>

Download/MMP

5. NGINX NGINX JavaScript 模块缓冲区错误漏洞 (CNNVD-202202-1182)

NGINX是美国NGINX公司的一款轻量级Web服务器/反向代理服务
器。

NGINX JavaScript (njs) 模块存在缓冲区错误漏洞，该漏洞源
于/src/njs_vmcode.c中函数njs_vmcode_typeof存在越界访问数组。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://github.com/nginx/njs/commit/d457c9545e7e71ebb5c0479eb16b9d33175855e2>

6.Schneider Electric Interactive Graphical SCADA System Data Collector访问控制错误漏洞 (CNNVD-202202-1051)

Schneider Electric Interactive Graphical SCADA System (IGSS) 是
法国施耐德电气 (Schneider Electric) 公司的一套用于监控和控制工
业过程的SCADA (数据采集与监控系统) 系统。

IGSS Data Collector 模块存在访问控制错误漏洞，该漏洞源于缺
少对网络消息的验证。攻击者利用该漏洞会导致删除任意文件

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-20

21-348-01

7. NGINX NGINX JavaScript 模块资源管理错误漏洞 (CNNVD-202202-1196)

NGINX是美国NGINX公司的一款轻量级Web服务器/反向代理服务
器。

NGINX JavaScript (njs) 模块存在资源管理错误漏洞，该漏洞
源于在njs_await_fulfilled函数中包含内存释放后引用问题。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

[https://github.com/nginx/njs/commit/6a07c2156a07ef307b6dcf3c2ca
8571a5f1af7a6](https://github.com/nginx/njs/commit/6a07c2156a07ef307b6dcf3c2ca8571a5f1af7a6)

8. Schneider Electric Interactive Graphical SCADA System Data Server 输入验证错误漏洞 (CNNVD-202202-909)

Schneider Electric Interactive Graphical SCADA System (IGSS) 是
法国施耐德电气 (Schneider Electric) 公司的一套用于监控和控制工
业过程的SCADA (数据采集与监控系统) 系统。

IGSS Data Server存在输入验证错误漏洞，该漏洞可导致堆缓冲
区溢出。攻击者利用该漏洞发送多个专门制作的消息会导致拒绝服务
和远程代码执行。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

[https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-20
22-039-01](https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-039-01)

1.4.2 高危漏洞实例

2022年2月高危漏洞共698个，其中重要漏洞实例如表6所示。

表6 2022年2月高危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例	
SQL注入	Airspan Networks	CNNVD-202202-202	SAP NetWeaver AS ABAP SQL注入漏洞 (CNNVD-202202-558)	
	Packet Tide	CNNVD-202202-1582		
	SAP	CNNVD-202202-558		
	The Cyrus Team团队	CNNVD-202202-1766		
	Unified Office	CNNVD-202202-152		
	WordPress基金会			CNNVD-202202-053
				CNNVD-202202-366
				CNNVD-202202-976
				CNNVD-202202-1127
				CNNVD-202202-1682
				CNNVD-202202-1685
				CNNVD-202202-1691
	个人开发者			CNNVD-202202-1697
				CNNVD-202202-151
				CNNVD-202202-212
				CNNVD-202202-975
				CNNVD-202202-1282
				CNNVD-202202-1382
		CNNVD-202202-1640		
代码问题	Acronis	CNNVD-202202-1820	Apache Cayenne 代码问题漏洞 (CNNVD-202202-1031)	
		CNNVD-202202-364		
		CNNVD-202202-365		
	Adobe	CNNVD-202202-1059		
		CNNVD-202202-626		
	Airspan Networks	CNNVD-202202-197		
	Amd	CNNVD-202202-340		
	Apache基金会	CNNVD-202202-445		
		CNNVD-202202-1031		
	Atlassian	CNNVD-202202-1257		
	Axis	CNNVD-202202-1192		
	Django基金会	CNNVD-202202-022		
	Gitea社区	CNNVD-202202-728		
	Google	CNNVD-202202-475		
	Insyde	CNNVD-202202-116		
Intel	CNNVD-202202-747			
	CNNVD-202202-758			

		CNNVD-202202-759		
	Jenkins	CNNVD-202202-771		
	Linux基金会	CNNVD-202202-1027		
	MODX	CNNVD-202202-2089		
	MariaDB基金会			CNNVD-202202-001
				CNNVD-202202-002
				CNNVD-202202-003
				CNNVD-202202-004
				CNNVD-202202-005
	Mozilla基金会	CNNVD-202202-2072		
	OIC	CNNVD-202202-906		
	Qualcomm	CNNVD-202202-488		
	Shibboleth	CNNVD-202202-332		
	Siemens	CNNVD-202202-801		
	Trigone	CNNVD-202202-1391		
	ocProducts	CNNVD-202202-782		
	个人开发者			CNNVD-202202-140
				CNNVD-202202-375
				CNNVD-202202-516
				CNNVD-202202-741
		CNNVD-202202-742		
		CNNVD-202202-746		
		CNNVD-202202-765		
		CNNVD-202202-921		
		CNNVD-202202-1209		
		CNNVD-202202-1211		
		CNNVD-202202-1357		
		CNNVD-202202-1652		
		CNNVD-202202-1658		
	CNNVD-202202-1759			
	CNNVD-202202-1788			
授权问题	Capsule8	CNNVD-202202-137	Capsule8 Capsule8 控制台 授权问题漏洞 (CNNVD-202202-137)	
	HP			CNNVD-202202-1330
				CNNVD-202202-1331
				CNNVD-202202-1332
				CNNVD-202202-1334
		CNNVD-202202-1335		
	JqueryForm.com	CNNVD-202202-1376		
	Sealevel Systems			CNNVD-202202-344
		CNNVD-202202-346		
Siemens	CNNVD-202202-592			
StarWind	CNNVD-202202-448			

	TOTOLink	CNNVD-202202-250	
	Zzcms团队	CNNVD-202202-1155	
	个人开发者	CNNVD-202202-031	
		CNNVD-202202-1753	
		CNNVD-202202-1756	
操作系统 命令注入	Apache基金会	CNNVD-202202-1940	Fortinet FortiWeb 操作系统命令注入漏洞 (CNNVD-202202-129)
	Cisco	CNNVD-202202-1790	
	Elecom	CNNVD-202202-602	
	Fortinet	CNNVD-202202-129	
		CNNVD-202202-136	
	Microweber社区	CNNVD-202202-1029	
	Synology	CNNVD-202202-511	
	VMware	CNNVD-202202-1273	
	Zyxel	CNNVD-202202-1780	
	个人开发者	CNNVD-202202-1108	
CNNVD-202202-1260			
CNNVD-202202-1287			
CNNVD-202202-1288			
缓冲区错 误	Adobe	CNNVD-202202-623	Cisco Small Business RV 系列路由器 缓冲区错误漏洞 (CNNVD-202202-164)
		CNNVD-202202-662	
		CNNVD-202202-672	
		CNNVD-202202-704	
	Cisco	CNNVD-202202-163	
		CNNVD-202202-164	
		CNNVD-202202-167	
		CNNVD-202202-169	
		CNNVD-202202-171	
	Eclipse基金会	CNNVD-202202-033	
	FATEK	CNNVD-202202-1932	
		CNNVD-202202-1934	
	Foxit	CNNVD-202202-932	
		CNNVD-202202-936	
		CNNVD-202202-945	
		CNNVD-202202-948	
		CNNVD-202202-1037	
	Google	CNNVD-202202-185	
		CNNVD-202202-189	
		CNNVD-202202-192	
CNNVD-202202-193			
CNNVD-202202-393			
CNNVD-202202-394			
CNNVD-202202-399			
CNNVD-202202-404			

		CNNVD-202202-424
		CNNVD-202202-426
		CNNVD-202202-468
		CNNVD-202202-472
		CNNVD-202202-473
		CNNVD-202202-1054
		CNNVD-202202-1067
	Hancom	CNNVD-202202-1336
	Insyde	CNNVD-202202-102
		CNNVD-202202-104
		CNNVD-202202-105
		CNNVD-202202-112
		CNNVD-202202-113
		CNNVD-202202-115
		CNNVD-202202-117
	Intel	CNNVD-202202-641
		CNNVD-202202-642
		CNNVD-202202-748
	KiCad社区	CNNVD-202202-177
		CNNVD-202202-178
		CNNVD-202202-1353
		CNNVD-202202-1354
	Linux基金会	CNNVD-202202-179
		CNNVD-202202-542
		CNNVD-202202-543
		CNNVD-202202-1378
	Mediatek	CNNVD-202202-881
	Mozilla基金会	CNNVD-202202-569
		CNNVD-202202-591
		CNNVD-202202-1278
	Qualcomm	CNNVD-202202-501
	Santesoft	CNNVD-202202-154
		CNNVD-202202-155
		CNNVD-202202-156
		CNNVD-202202-157
		CNNVD-202202-161
		CNNVD-202202-162
	Schneider Electric	CNNVD-202202-382
		CNNVD-202202-913
		CNNVD-202202-915
		CNNVD-202202-1045
		CNNVD-202202-1052
	Sealevel Systems	CNNVD-202202-098

		CNNVD-202202-347
		CNNVD-202202-348
	Siemens	CNNVD-202202-809
		CNNVD-202202-810
		CNNVD-202202-811
		CNNVD-202202-816
		CNNVD-202202-818
		CNNVD-202202-820
		CNNVD-202202-822
		CNNVD-202202-824
		CNNVD-202202-825
		CNNVD-202202-827
		CNNVD-202202-829
		CNNVD-202202-830
		CNNVD-202202-831
		CNNVD-202202-1403
		TOTOLink
	CNNVD-202202-247	
	CNNVD-202202-249	
	CNNVD-202202-251	
	CNNVD-202202-253	
	CNNVD-202202-255	
	TP-Link	CNNVD-202202-941
		CNNVD-202202-943
		CNNVD-202202-944
		CNNVD-202202-1851
	Tenda	CNNVD-202202-213
		CNNVD-202202-214
		CNNVD-202202-215
		CNNVD-202202-216
		CNNVD-202202-217
		CNNVD-202202-218
		CNNVD-202202-219
		CNNVD-202202-220
		CNNVD-202202-221
		CNNVD-202202-222
		CNNVD-202202-224
		CNNVD-202202-225
		CNNVD-202202-227
		CNNVD-202202-229
CNNVD-202202-232		
CNNVD-202202-260		
CNNVD-202202-261		

		CNNVD-202202-263		
		CNNVD-202202-264		
		CNNVD-202202-265		
		CNNVD-202202-266		
		CNNVD-202202-268		
		CNNVD-202202-269		
		CNNVD-202202-270		
		CNNVD-202202-288		
		CNNVD-202202-290		
		CNNVD-202202-292		
		CNNVD-202202-293		
		CNNVD-202202-294		
		CNNVD-202202-295		
		CNNVD-202202-298		
		CNNVD-202202-300		
		CNNVD-202202-1151		
		CNNVD-202202-1325		
		WatchGuard		CNNVD-202202-1839
				CNNVD-202202-1840
				CNNVD-202202-1844
	Wireshark团队	CNNVD-202202-1191		
	个人开发者	CNNVD-202202-469		
		CNNVD-202202-735		
		CNNVD-202202-736		
		CNNVD-202202-739		
		CNNVD-202202-740		
		CNNVD-202202-865		
		CNNVD-202202-1372		
		CNNVD-202202-1399		
		CNNVD-202202-1655		
		CNNVD-202202-1725		
		CNNVD-202202-1729		
		CNNVD-202202-1754		
		CNNVD-202202-1791		
访问控制 错误	Citrix Systems	CNNVD-202202-888	VMware ESXi 访问控制错误漏洞 (CNNVD-202202-1225)	
	Intel	CNNVD-202202-631		
		CNNVD-202202-685		
		CNNVD-202202-753		
				CNNVD-202202-755
	JetBrains	CNNVD-202202-605		
	Librenms社区	CNNVD-202202-1197		
VMware	CNNVD-202202-1225			
	WatchGuard	CNNVD-202202-1837		

	WordPress基金会	CNNVD-202202-530	
	个人开发者	CNNVD-202202-545	
		CNNVD-202202-716	
		CNNVD-202202-722	
		CNNVD-202202-1676	
		CNNVD-202202-1679	
		CNNVD-202202-2048	
资源管理 错误	Apache基金会	CNNVD-202202-257	Cisco NX-OS Software 资源管理错误漏洞 (CNNVD-202202-1783)
	Cisco	CNNVD-202202-1783	
		CNNVD-202202-1794	
	Foxit	CNNVD-202202-931	
		CNNVD-202202-933	
		CNNVD-202202-934	
		CNNVD-202202-935	
		CNNVD-202202-938	
		CNNVD-202202-947	
		CNNVD-202202-949	
		CNNVD-202202-950	
		CNNVD-202202-951	
		Google	
	CNNVD-202202-024		
	CNNVD-202202-027		
	CNNVD-202202-056		
	CNNVD-202202-063		
	CNNVD-202202-417		
	CNNVD-202202-419		
	CNNVD-202202-477		
	CNNVD-202202-928		
	CNNVD-202202-1153		
	CNNVD-202202-1180		
	CNNVD-202202-1186		
	CNNVD-202202-1190		
	CNNVD-202202-1201		
	Iobit	CNNVD-202202-1593	
	MariaDB基金会	CNNVD-202202-008	
		CNNVD-202202-011	
	Mediatek	CNNVD-202202-768	
		CNNVD-202202-872	
	Qualcomm	CNNVD-202202-885	
CNNVD-202202-497			
SAP	CNNVD-202202-557		
	CNNVD-202202-890		
Santesoft	CNNVD-202202-159		

	Schneider Electric	CNNVD-202202-383		
	StarWind	CNNVD-202202-446		
	VMware	CNNVD-202202-1206		
	WordPress基金会	CNNVD-202202-1133		
	php	CNNVD-202202-1398		
	个人开发者			CNNVD-202202-037
				CNNVD-202202-148
				CNNVD-202202-734
				CNNVD-202202-738
				CNNVD-202202-886
				CNNVD-202202-955
				CNNVD-202202-1038
				CNNVD-202202-1280
		CNNVD-202202-1722		
	CNNVD-202202-1764			
输入验证 错误	ABB	CNNVD-202202-350	Mirantis Mirantis Container Cloud 输入验证错误漏洞 (CNNVD-202202-376)	
		CNNVD-202202-352		
	Cisco	CNNVD-202202-1314		
	Drupal社区	CNNVD-202202-1377		
	Google			CNNVD-202202-191
				CNNVD-202202-391
				CNNVD-202202-392
				CNNVD-202202-395
				CNNVD-202202-421
				CNNVD-202202-1173
	Intel			CNNVD-202202-651
				CNNVD-202202-669
				CNNVD-202202-675
				CNNVD-202202-681
				CNNVD-202202-687
				CNNVD-202202-689
		CNNVD-202202-754		
	Kde社区	CNNVD-202202-549		
	MariaDB基金会			CNNVD-202202-007
				CNNVD-202202-766
	CNNVD-202202-769			
Microsoft	CNNVD-202202-698			
Mirantis	CNNVD-202202-376			
Qualcomm		CNNVD-202202-493		
		CNNVD-202202-494		
Samsung	CNNVD-202202-1066			
Schneider Electric		CNNVD-202202-384		
		CNNVD-202202-1044		

		CNNVD-202202-1048
	Sealevel Systems	CNNVD-202202-099
	Siemens	CNNVD-202202-550
		CNNVD-202202-551
		CNNVD-202202-568
	TP-Link	CNNVD-202202-1109
	Tobesoft	CNNVD-202202-900
	Trend Micro	CNNVD-202202-1739
	VMware	CNNVD-202202-1207
	个人开发者	CNNVD-202202-517
		CNNVD-202202-547
		CNNVD-202202-548
		CNNVD-202202-594
		CNNVD-202202-923
		CNNVD-202202-1422
		CNNVD-202202-1606
		CNNVD-202202-2141

1.SAP NetWeaver AS ABAP SQL注入漏洞（CNNVD-202202-558）

SAP NetWeaver AS ABAP是德国思爱普（SAP）公司的一款高级商务应用开发环境服务器，是SAP NetWeaver开发商务应用平台的一部分。

SAP NetWeaver AS ABAP存在SQL注入漏洞，以下版本受影响：700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

<https://vigilance.fr/vulnerability/SAP-multiple-vulnerabilities-de-decembre-2021-37478>

2.Apache Cayenne 代码问题漏洞（CNNVD-202202-1031）

Apache Cayenne是美国阿帕奇（Apache）基金会的一款提供对象关系映射（ORM）和远程服务的开源持久性框架。

Apache Cayenne存在代码问题漏洞，该漏洞源于产品未对用户上

传的负载进行安全检查。攻击者可通过该漏洞导致任意代码执行。以下产品及版本受到影响：Apache Cayenne 4.1 版本及之前版本。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://lists.apache.org/thread/zthjy83t3o66x7xcbygn2vg3yjlvc9vc>

3. Capsule8 Capsule8 控制台授权问题漏洞(CNNVD-202202-137)

Capsule8 是美国Capsule8 公司的一套针对Linux的实时攻击检测平台。

Capsule8 控制台存在授权问题漏洞，该漏洞源于经过身份验证和授权的代理用户可以通过对Capsule8 Console SQLi漏洞获得管理访问权限。以下产品及版本受到影响：Capsule8 控制台 4.6.0 和 4.9.1 版本之间。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.sophos.com/en-us/security-advisories/sophos-sa-20220201-cap8-console-sqli>

4. Fortinet FortiWeb 操作系统命令注入漏洞 (CNNVD-202202-129)

Fortinet FortiWeb是美国飞塔（Fortinet）公司的一款Web应用层防火墙，它能够阻断如跨站点脚本、SQL注入、Cookie中毒、schema中毒等攻击的威胁，保证Web应用程序的安全性并保护敏感的数据库内容。

Fortinet FortiWeb 6.15 和 6.15 和 6.0.6.3 和 6.0 Web 3、6.2.4 和 6.2 存在操作系统命令注入漏洞，该漏洞源于产品未对用户发起

的HTTP请求数据中的内容进行有效验证。攻击者利用该漏洞可执行任意命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://fortiguard.com/psirt/FG-IR-21-158>

5. Cisco Small Business RV 系列路由器缓冲区错误漏洞 (CNNVD-202202-164)

Cisco Small Business RV 系列路由器是美国思科（Cisco）公司的多款专为小型企业设计的简单、灵活且高度安全的网络路由设备。

Cisco Small Business RV系列路由器存在缓冲区错误漏洞，该漏洞源于安装在受影响设备上的软件映像验证不当所致。攻击者利用该漏洞可安装和启动恶意软件映像或在设备上执行未签名的二进制文件。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-smb-mult-vuln-KA9PK6D>

6. VMware ESXi 访问控制错误漏洞 (CNNVD-202202-1225)

VMware ESXi是美国威睿（VMware）公司的一套可直接安装在物理服务器上的服务器虚拟化平台。

VMWare ESXi中存在访问控制错误漏洞，该漏洞源于VMX有权访问settingsd授权票证，VMX进程中具有特权的攻击者能够访问以高权限用户身份运行的settingsd服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.vmware.com/security/advisories/VMSA-2022-0004.html>

7.Cisco NX-OS Software 资源管理错误漏洞 (CNNVD-202202-1783)

Cisco NX-OS Software是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。

Cisco NX-OS Software 存在资源管理错误漏洞，该漏洞源于Cisco NX-OS Software的Cisco Fabric Services over IP (CFSoIP) 功能对传入 CFSoIP 数据包的验证不足。攻击者利用该漏洞在受影响的设备上造成拒绝服务。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisor/cisco-sa-cfsoip-dos-tpykyDr>

8.Mirantis Mirantis Container Cloud 输入验证错误漏洞 (CNNVD-202202-376)

Mirantis Container Cloud是美国Mirantis公司的一个容器平台，支持基于任何基础架构进行Kubernetes集群部署和管理。

Mirantis Container Cloud存在输入验证错误漏洞，该漏洞源于缺少 URL 验证。该漏洞影响 3.1.1 之前版本的 Mirantis Container Cloud Lens Extension。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://github.com/Mirantis/security/blob/main/advisories/0005.md>

二、漏洞平台推送情况

2022年2月漏洞平台推送漏洞4435个。

表7 2022年2月漏洞平台推送情况表

序号	漏洞平台	漏洞总量
1	漏洞盒子	2735
2	补天平台	1600
推送总计		4335

三、接报漏洞情况

2022年2月接报漏洞1796个，其中信息技术产品漏洞（通用型漏洞）272个，网络信息系统漏洞（事件型漏洞）1524个。

表8 2022年2月接报漏洞情况表

序号	报送单位	漏洞数量
1	北京安全共识科技有限公司	859
2	西安四叶草信息技术有限公司	168
3	北京国舜科技股份有限公司	114
4	南京众智维信息科技有限公司	80
5	山东新潮信息技术有限公司	71
6	北京永信至诚科技股份有限公司	33
7	北京网御星云信息技术有限公司	33
8	杭州海康威视数字技术股份有限公司	30
9	广州易东信息安全技术有限公司	25
10	杭州安恒信息技术股份有限公司	23
11	北京天融信网络安全技术有限公司	22
12	北京微步在线科技有限公司	21
13	北京数字观星科技有限公司	21
14	星云博创科技有限公司	20
15	远江盛邦（北京）网络安全科技股份有限公司	20
16	北京山石网科信息技术有限公司	20
17	广州竞远安全技术股份有限公司	20
18	山东泽鹿安全技术有限公司	16
19	北京安盟信息技术股份有限公司	15
20	华为技术有限公司	14
21	南京禾盾信息科技有限公司	13
22	上海安几科技有限公司	12
23	浪潮电子信息产业股份有限公司	11

24	北京华云安信息技术有限公司	11
25	北京云测信息技术有限公司	10
26	北京安华金和科技有限公司	9
27	杭州迪普科技股份有限公司	8
28	上海上讯信息技术股份有限公司	8
29	新华三技术有限公司	8
30	长春嘉诚信息技术股份有限公司	7
31	杭州默安科技有限公司	7
32	个人	7
33	中兴通讯股份有限公司	6
34	上海安识网络科技有限公司	6
35	北京世纪先承信息安全科技有限公司	5
36	厦门服云信息科技有限公司	4
37	中国电信集团系统集成有限责任公司	4
38	腾讯科技（北京）有限公司	4
39	百度公司	4
40	海南神州希望网络有限公司	4
41	亚信科技（成都）有限公司	3
42	深圳融安网络科技有限公司	2
43	河南听潮盛世信息技术有限公司	2
44	北京威努特技术有限公司	2
45	北京机沃科技有限公司	2
46	北京奇虎科技有限公司	1
47	战略支援部队信息工程大学	1
48	三六零数字安全科技集团有限公司	1
49	北京安帝科技有限公司	1
50	恒安嘉新（北京）科技股份公司	1
51	北京华顺信安科技有限公司	1
52	中国电信股份有限公司研究院	1
53	中电云数智科技有限公司	1
54	上海斗象信息科技有限公司	1
55	北京华胜久安科技有限公司	1
56	北京智游网安科技有限公司	1
57	中通服咨询设计研究院有限公司	1
报送合计		1796

四、重大漏洞预警

4.1 Fortinet FortiWeb 安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于Fortinet FortiWeb安全漏洞（CNNVD-202202-129、CVE-2021-43073）情况的报送。成功利用漏洞的攻击者，可向目标设备发送特殊请求，从而远程执行恶意代码。FortiWeb 6.4.1 及其以下版本均受此漏洞影响。目前，Fortinet官方已发布新版本修复了该漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

· 漏洞介绍

Fortinet FortiWeb是美国飞塔（Fortinet）公司的一款Web应用层防火墙，它能够阻断跨站点脚本、SQL注入、Cookie中毒等攻击的威胁，保证Web应用程序的安全性并保护敏感的数据库内容。漏洞源于FortiWeb对系统命令中的特殊元素处理不正确导致，攻击者可通过发送恶意HTTP 请求，对目标设备远程执行代码。

· 危害影响

成功利用漏洞的攻击者，可向目标设备发送特殊请求，从而远程执行恶意代码。FortiWeb 6.4.1 及其以下版本均受此漏洞影响。

· 修复建议

目前，Fortinet 官方已发布新版本修复了该漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

<https://fortiguard.com/psirt/FG-IR-21-158>

4.2 微软多个安全漏洞的预警

近日，微软官方发布了多个安全漏洞的公告，包括Microsoft Hyper-V 权限许可和访问控制问题漏洞（CNNVD-202201-787、CVE-2022-21901）、Microsoft Edge 代码注入漏洞（CNNVD-202202-235、CVE-2022-23263）等 58 个漏洞。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据，提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

· 漏洞介绍

2022 年 2 月 8 日，微软发布了 2022 年 2 月份安全更新，共 58 个漏洞的补丁程序，CNNVD对这些漏洞进行了收录。本次更新主要涵盖了Microsoft Windows 和 Windows 组件、Microsoft Edge、Microsoft Hyper-V、Microsoft Windows Print Spooler Components、Microsoft Visual Studio、Microsoft OneDrive等。CNNVD对其危害等级进行了评价，其中超危漏洞 1 个，高危漏洞 41 个，中危漏洞 16 个。微软多个产品和系统版本受漏洞影响，具体影响范围可访问 <https://portal.msrc.microsoft.com/zh-cn/security-guidance> 查询。

· 漏洞详情

此次更新共包括 58 个漏洞的补丁程序，其中超危漏洞 1 个，高危漏洞 41 个，中危漏洞 16 个。

序号	漏洞名称	CNNVD 编号	CVE 编号	危害等级	官方链接
1	Microsoft Hyper-V 权限许可和访问控制问题漏洞	CNNVD-202201-787	CVE-2022-21901	超危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21901
2	Microsoft Edge 代码注入漏洞	CNNVD-202202-235	CVE-2022-23263	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23263
3	Microsoft Office 代码注入漏洞	CNNVD-202202-572	CVE-2022-22004	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22004
4	Microsoft Office 代码注入漏洞	CNNVD-202202-580	CVE-2022-22005	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22005
5	Microsoft Office 代码注入漏洞	CNNVD-202202-582	CVE-2022-22003	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22003

6	Microsoft Office 代码注入漏洞	CNNVD-2022-583	CVE-2022-21988	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21988
7	Microsoft Office 安全漏洞	CNNVD-2022-586	CVE-2022-21987	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21987
8	Microsoft Windows Print Spooler Components 权限许可和访问控制问题漏洞	CNNVD-2022-595	CVE-2022-22718	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22718
9	Microsoft Windows Print Spooler Components 权限许可和访问控制问题漏洞	CNNVD-2022-596	CVE-2022-22717	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22717
10	Microsoft Windows 权限许可和访问控制问题漏洞	CNNVD-2022-599	CVE-2022-22715	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22715

11	Microsoft Windows DNS 代码注入漏洞	CNNVD-2022-607	CVE-2022-21984	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984
12	Microsoft Windows Common Log File System Driver 权限许可和访问控制问题漏洞	CNNVD-2022-609	CVE-2022-21981	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21981
13	Microsoft Windows Remote Access Connection Manager 权限许可和访问控制问题漏洞	CNNVD-2022-611	CVE-2022-22001	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22001
14	Microsoft Windows Common Log File System Driver 权限许可和访问控制问题漏洞	CNNVD-2022-612	CVE-2022-22000	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22000
15	Microsoft Windows Kernel 权限许可和访问控制问题漏洞	CNNVD-2022-614	CVE-2022-21989	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21989

16	Microsoft Visual Studio 代码注入漏洞	CNNVD-2022-616	CVE-2022-21991	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21991
17	Microsoft Windows Mobile Device Management 代码注入漏洞	CNNVD-2022-617	CVE-2022-21992	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21992
18	Microsoft Windows Kernel 信息泄露漏洞	CNNVD-2022-618	CVE-2022-21993	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21993
19	Microsoft DWM Core Library 权限许可和访问控制问题漏洞	CNNVD-2022-619	CVE-2022-21994	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21994
20	Microsoft Windows Print Spooler Components 权限许可和访问控制问题漏洞	CNNVD-2022-620	CVE-2022-21999	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999

21	Microsoft Hyper-V 代码注入漏洞	CNNVD-2022-621	CVE-2022-21995	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21995
22	Microsoft Windows Print Spooler Components 权限许可和访问控制问题漏洞	CNNVD-2022-622	CVE-2022-21997	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21997
23	Microsoft Win32k 权限许可和访问控制问题漏洞	CNNVD-2022-624	CVE-2022-21996	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21996
24	Microsoft Windows Runtime 代码注入漏洞	CNNVD-2022-625	CVE-2022-21971	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21971
25	Microsoft Dynamics 代码注入漏洞	CNNVD-2022-627	CVE-2022-23274	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23274

26	Microsoft Dynamics 权限许可和访问控制问题漏洞	CNNVD-2022-628	CVE-2022-23273	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23273
27	Microsoft Dynamics 权限许可和访问控制问题漏洞	CNNVD-2022-636	CVE-2022-23272	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23272
28	Microsoft Azure 安全漏洞	CNNVD-2022-639	CVE-2022-23256	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23256
29	Microsoft SQL Server 权限许可和访问控制问题漏洞	CNNVD-2022-668	CVE-2022-23276	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23276
30	Microsoft Roaming Security Rights Management Services 代码注入漏洞	CNNVD-2022-676	CVE-2022-21974	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21974

31	Microsoft Windows Codecs Library 代码注入漏洞	CNNVD-2022-688	CVE-2022-21844	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21844
32	Microsoft Windows Codecs Library 代码注入漏洞	CNNVD-2022-691	CVE-2022-21926	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21926
33	Microsoft Windows Codecs Library 代码注入漏洞	CNNVD-2022-694	CVE-2022-21927	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21927
34	Microsoft Dynamics 代码注入漏洞	CNNVD-2022-696	CVE-2022-21957	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21957
35	Microsoft Teams 输入验证错误漏洞	CNNVD-2022-698	CVE-2022-21965	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21965

36	Microsoft Windows Codecs Library 代码注入漏洞	CNNVD-2022-701	CVE-2022-22709	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22709
37	Microsoft Graphics Components 安全漏洞	CNNVD-2022-785	CVE-2022-21903	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21903
38	Microsoft Windows Common Log File System Driver 缓冲区错误漏洞	CNNVD-2022-789	CVE-2022-21897	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21897
39	Microsoft Windows 安全漏洞	CNNVD-2022-790	CVE-2022-21896	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21896
40	Microsoft Windows 缓冲区错误漏洞	CNNVD-2022-791	CVE-2022-21895	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21895

41	多款 Microsoft 产品安全 漏洞	CNNVD-20 2201-795	CVE-2022 -21893	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21893
42	Microsoft Windows DirectX 安 全漏洞	CNNVD-20 2201-788	CVE-2022 -21898	高危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21898
43	Microsoft Edge 代码 注入漏洞	CNNVD-20 2202-236	CVE-2022 -23262	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23262
44	Microsoft Edge 安全 漏洞	CNNVD-20 2202-237	CVE-2022 -23261	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23261
45	Microsoft Office 信 息泄露漏 洞	CNNVD-20 2202-570	CVE-2022 -23252	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23252

46	Microsoft Office 信息泄露漏洞	CNNVD-2022-573	CVE-2022-22716	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22716
47	Microsoft Office 安全特征问题特征问题漏洞	CNNVD-2022-574	CVE-2022-23280	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23280
48	Microsoft Office 安全特征问题漏洞	CNNVD-2022-581	CVE-2022-21968	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21968
49	Microsoft Hyper-V 输入验证错误漏洞	CNNVD-2022-598	CVE-2022-22712	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22712
50	Microsoft Windows Common Log File System Driver 输入验证错误漏洞	CNNVD-2022-604	CVE-2022-22710	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22710

51	Microsoft Windows 输入验证错误漏洞	CNNVD-2022-610	CVE-2022-22002	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22002
52	Microsoft Windows Common Log File System Driver 信息泄露漏洞	CNNVD-2022-613	CVE-2022-21998	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21998
53	Microsoft Windows Remote Access Connection Manager 信息泄露漏洞	CNNVD-2022-615	CVE-2022-21985	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21985
54	Microsoft Dynamics 权限许可和访问控制问题漏洞	CNNVD-2022-630	CVE-2022-23271	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23271
55	Microsoft Dynamics 安全漏洞	CNNVD-2022-632	CVE-2022-23269	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23269

56	Microsoft Power BI 权限许可和访问控制问题漏洞	CNNVD-2022-706	CVE-2022-23254	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23254
57	Microsoft OneDrive 安全特征问题漏洞	CNNVD-2022-711	CVE-2022-23255	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23255
58	Microsoft .NET Core 和 Microsoft Visual Studio 信息泄露漏洞	CNNVD-2021-799	CVE-2021-41355	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41355

修复建议

目前，微软官方已经发布补丁修复了上述漏洞，建议用户及时确认漏洞影响，尽快采取修补措施。微软官方补丁下载地址：

<https://msrc.microsoft.com/update-guide/en-us>