

北京师范大学网络信息安全通告

2022 年 6 月报告

北京师范大学信息网络中心

2022 年 7 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.....	6
1.3.1. 整体修复情况	6
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	16
2. 漏洞平台推送情况.....	30
3. 接报漏洞情况.....	30
4. 重大漏洞预警.....	32
4.1. Microsoft Windows Support Diagnostic Tool 安全漏洞的通报.....	32
4.2. 微软多个安全漏洞的通报.....	35

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6月份新增安全漏洞共2346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200个；从漏洞类型来看，跨站脚本类的漏洞占比最大，达到13.17%。本月新增漏洞中，超危漏洞397个、高危漏洞865个、中危漏洞1027个、低危漏洞57个，相应修复率分别为66.50%、64.97%、79.65%以及78.95%。合计1689个漏洞已有修复补丁发布，本月整体修复率71.99%。

截至2022年06月30日，CNNVD采集漏洞总量已达187130个。

1.1 漏洞增长概况

2022年6月新增安全漏洞2346个，与上月（2044个）相比增加了14.77%。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2078个。

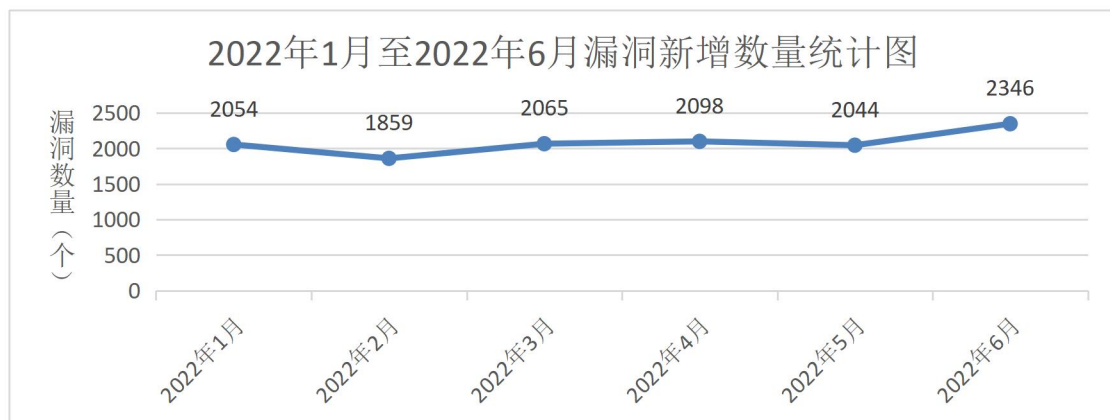


图1 2022年1月至2022年6月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2022年6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200个，占本月漏洞总量的8.53%。

表1 2022年6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	200	8.53%
2	Google	101	4.31%
3	Microsoft	62	2.64%
4	Adobe	50	2.13%
5	IBM	41	1.75%
6	Samsung	41	1.75%
7	Siemens	29	1.24%
8	PHP	25	1.07%
9	Qualcomm	24	1.02%
10	Dell	23	0.98%

1.2.2 漏洞产品分布

2022年6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40个¹，Android漏洞数量最多，共83个，占主流操作系统漏洞总量的21.34%，排名第一。

表2 2022年6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	83
2	Windows Server 2019	30
3	Windows Server 2022	29
4	Windows Server 2016	29

¹ Windows系列操作系统多个版本可能同时受同一个漏洞影响。

5	Windows 10	28
6	Windows 11	27
7	Windows Server 2012	24
8	Windows Server 2012 R2	24
9	Windows 8.1	22
10	Windows Rt 8.1	21
11	Windows Server 2008	20
12	Windows Server 2008 R2	20
13	Windows 7	20
14	Linux Kernel	12

1.2.3 漏洞类型分布

2022年6月份发布的漏洞类型分布如表3所示，其中跨站脚本类漏洞所占比例最大，约为13.17%。

表3 2022年6月漏洞类型统计表

序号	漏洞类型	漏洞数量(个)	所占比例
1	跨站脚本	309	13.17%
2	SQL注入	302	12.87%
3	缓冲区错误	197	8.40%
4	跨站请求伪造	110	4.69%
5	代码问题	109	4.65%
6	输入验证错误	74	3.15%
7	资源管理错误	69	2.94%
8	信息泄露	48	2.05%
9	授权问题	44	1.88%
10	操作系统命令注入	40	1.71%
11	路径遍历	33	1.41%
12	信任管理问题	26	1.11%
13	访问控制错误	24	1.02%
14	命令注入	20	0.85%
15	安全特征问题	18	0.77%
16	数据伪造问题	17	0.72%
17	代码注入	15	0.64%
18	权限许可和访问控制问题	11	0.47%
19	注入	11	0.47%
20	日志信息泄露	11	0.47%
21	竞争条件问题	7	0.30%

22	加密问题	5	0.21%
23	参数注入	5	0.21%
24	数字错误	4	0.17%
25	后置链接	3	0.13%
26	环境问题	2	0.09%
27	格式化字符串错误	1	0.04%
28	其他	831	35.42%

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6月漏洞危害等级分布如图2所示，其中超危漏洞397条，占本月漏洞总数的16.92%。

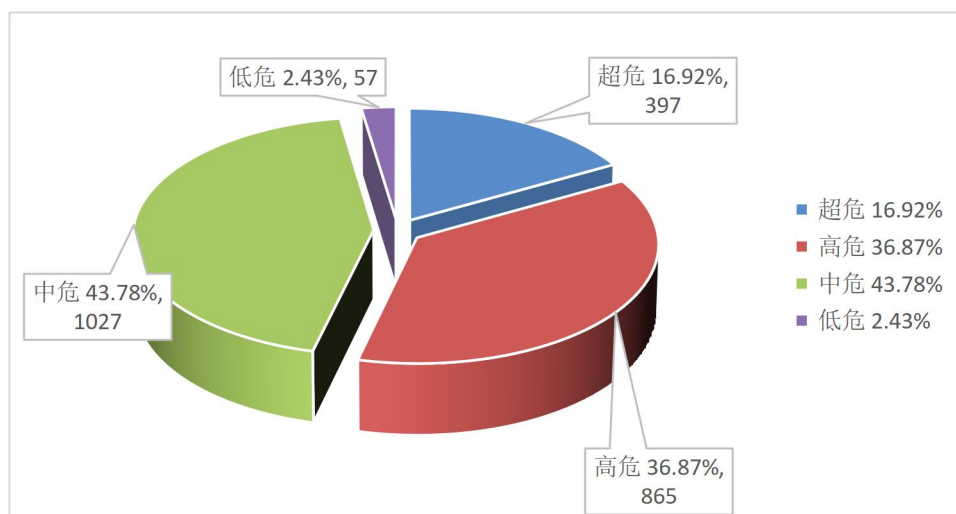


图2 2022年6月漏洞危害等级分布

1.3 漏洞修复情

1.3.1 整体修复情况

2022年6月漏洞修复情况按危害等级进行统计见图3。其中中危漏洞修复率最高,达到79.65%,高危漏洞修复率最低,比例为64.97%。

总体来看,本月整体修复率,由上月的78.33%下降至本月的71.99%。

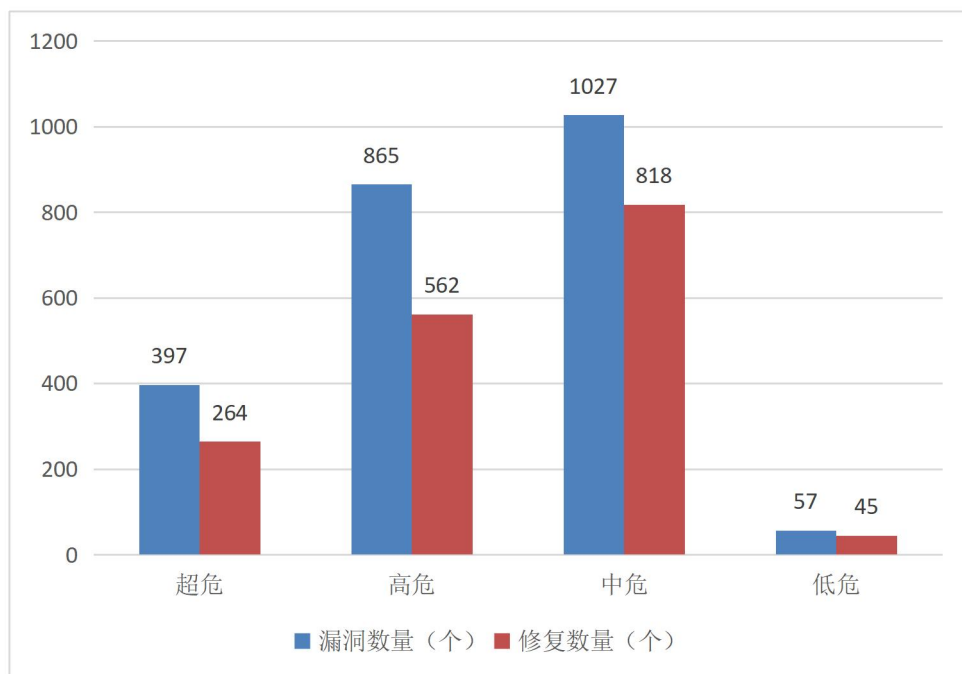


图3 2022年6月漏洞修复数量统计

1.3.2 厂商修复情况

2022年6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、Microsoft等十个厂商共596条漏洞,占本月漏洞总数的25.40%,漏洞修复率为89.93%,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

Adobe、Samsung、Siemens、Qualcomm 等公司本月漏洞修复率均为 100%，共 536 条漏洞已全部修复。

表 4 2022 年 6 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	200	166	83.00%
2	Google	101	97	96.04%
3	Microsoft	62	59	95.16%
4	Adobe	50	50	100.00%
5	IBM	41	40	97.56%
6	Samsung	41	41	100.00%
7	Siemens	29	29	100.00%
8	PHP	25	8	32.00%
9	Qualcomm	24	24	100.00%
10	Dell	23	22	95.65%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

2022 年 6 月超危漏洞共 397 个，其中重要漏洞实例如表 5 所示。

表 5 2022 年 6 月超危漏洞实例

漏洞类型	厂商	CNNVD 编号	漏洞实例
SQL 注入	ACEware Systems	CNNVD-202206-300	IBM InfoSphere Information Server SQL 注入漏洞 (CNNVD-202206-597)
	Advantech	CNNVD-202206-2713	
		CNNVD-202206-2714	
		CNNVD-202206-2717	
		CNNVD-202206-2731	
		CNNVD-202206-1168	
	Amodat	CNNVD-202206-1168	
	BrowsBox	CNNVD-202206-392	
	Docebo	CNNVD-202206-2300	
	EGavilan Media	CNNVD-202206-310	
		CNNVD-202206-311	
		CNNVD-202206-312	
	IBM	CNNVD-202206-597	
CNNVD-202206-1508			
Lógico y Creativo	CNNVD-202206-730		
Max Yi	CNNVD-202206-347		

		CNNVD-202206-2289	
	NOKIA	CNNVD-202206-1631	
	Neetai	CNNVD-202206-729	
	PHP Matrimonial Script	CNNVD-202206-2100	
	WordPress 基金会	CNNVD-202206-782	
		CNNVD-202206-801	
		CNNVD-202206-1133	
		CNNVD-202206-1137	
		CNNVD-202206-2033	
	elitecms	CNNVD-202206-222	
		CNNVD-202206-223	
		CNNVD-202206-224	
		CNNVD-202206-225	
		CNNVD-202206-227	
		CNNVD-202206-226	
	idea	CNNVD-202206-2290	
	phplist	CNNVD-202206-995	
		CNNVD-202206-1001	
	个人开发者	CNNVD-202206-142	
		CNNVD-202206-157	
		CNNVD-202206-158	
		CNNVD-202206-159	
		CNNVD-202206-162	
		CNNVD-202206-163	
		CNNVD-202206-168	
		CNNVD-202206-169	
		CNNVD-202206-170	
		CNNVD-202206-171	
		CNNVD-202206-172	
		CNNVD-202206-173	
		CNNVD-202206-174	
		CNNVD-202206-175	
		CNNVD-202206-177	
		CNNVD-202206-178	
		CNNVD-202206-180	
		CNNVD-202206-181	
		CNNVD-202206-182	
		CNNVD-202206-183	
	CNNVD-202206-184		
	CNNVD-202206-185		
	CNNVD-202206-187		

		CNNVD-202206-188	
		CNNVD-202206-189	
		CNNVD-202206-190	
		CNNVD-202206-191	
		CNNVD-202206-192	
		CNNVD-202206-194	
		CNNVD-202206-196	
		CNNVD-202206-197	
		CNNVD-202206-198	
		CNNVD-202206-199	
		CNNVD-202206-200	
		CNNVD-202206-201	
		CNNVD-202206-202	
		CNNVD-202206-221	
		CNNVD-202206-236	
		CNNVD-202206-238	
		CNNVD-202206-239	
		CNNVD-202206-242	
		CNNVD-202206-245	
		CNNVD-202206-247	
		CNNVD-202206-248	
		CNNVD-202206-272	
		CNNVD-202206-313	
		CNNVD-202206-350	
		CNNVD-202206-351	
		CNNVD-202206-352	
		CNNVD-202206-374	
		CNNVD-202206-376	
		CNNVD-202206-377	
		CNNVD-202206-379	
		CNNVD-202206-647	
		CNNVD-202206-728	
		CNNVD-202206-1002	
		CNNVD-202206-1027	
		CNNVD-202206-1043	
		CNNVD-202206-1044	
		CNNVD-202206-1083	
		CNNVD-202206-1204	
		CNNVD-202206-1205	
		CNNVD-202206-1293	
		CNNVD-202206-1314	

		CNNVD-202206-1324	
		CNNVD-202206-1481	
		CNNVD-202206-1493	
		CNNVD-202206-1602	
		CNNVD-202206-1603	
		CNNVD-202206-1604	
		CNNVD-202206-1681	
		CNNVD-202206-1686	
		CNNVD-202206-1700	
		CNNVD-202206-1701	
		CNNVD-202206-1703	
		CNNVD-202206-1715	
	五指	CNNVD-202206-1589	
代码问题	ACEware Systems	CNNVD-202206-302	Laravel 代码问题漏洞 (CNNVD-202206-671)
	ASG technologies	CNNVD-202206-1673	
	Chris Brame	CNNVD-202206-2071	
	Contec	CNNVD-202206-2116	
	IBM	CNNVD-202206-2072	
		CNNVD-202206-2073	
		CNNVD-202206-2507	
	Illumina	CNNVD-202206-386	
	Invision	CNNVD-202206-1185	
	Kreado	CNNVD-202206-1323	
	LaikeTui	CNNVD-202206-2286	
	Laravel	CNNVD-202206-671	
	Netscout	CNNVD-202206-405	
	Siemens	CNNVD-202206-116	
	Solar-Log	CNNVD-202206-968	
	WordPress 基金会	CNNVD-202206-2581	
	elitecms	CNNVD-202206-229	
	个人开发者	CNNVD-202206-250	
		CNNVD-202206-362	
		CNNVD-202206-387	
CNNVD-202206-902			
CNNVD-202206-906			
CNNVD-202206-1036			
CNNVD-202206-1495			
CNNVD-202206-1566			
CNNVD-202206-1583			
CNNVD-202206-2608			
极致网络科技	CNNVD-202206-903		

		CNNVD-202206-905	
	百度	CNNVD-202206-901	
	铭飞	CNNVD-202206-240	
	阿里巴巴	CNNVD-202206-1037	
授权问题	Axis	CNNVD-202206-1539	Siemens SIMATIC WinCC OA 授权问题漏洞 (CNNVD-202206-2079)
	Broadcom	CNNVD-202206-1654	
	Cisco	CNNVD-202206-1535	
		CNNVD-202206-1537	
	Exemys	CNNVD-202206-2902	
	IBM	CNNVD-202206-1716	
	IOBit	CNNVD-202206-1623	
	Klapp	CNNVD-202206-737	
	SiHAS	CNNVD-202206-2287	
	Siemens	CNNVD-202206-2079	
	Xi S&D	CNNVD-202206-2288	
	iSpyConnect	CNNVD-202206-2137	
	个人开发者	CNNVD-202206-1556	
CNNVD-202206-1706			
操作系统命令注入	Distributed Data Systems	CNNVD-202206-2946	TRENDnet TEW-831DR 操作系统命令注入漏洞 (CNNVD-202206-1664)
	Festo	CNNVD-202206-1154	
		CNNVD-202206-1155	
		CNNVD-202206-1156	
		CNNVD-202206-1158	
	Fujitsu	CNNVD-202206-2065	
		CNNVD-202206-2066	
	GOGS	CNNVD-202206-925	
	OpenNetAdmin	CNNVD-202206-935	
	OpenSSL	CNNVD-202206-2112	
	Robustel	CNNVD-202206-2891	
		CNNVD-202206-2892	
		CNNVD-202206-2893	
		CNNVD-202206-2894	
		CNNVD-202206-2895	
		CNNVD-202206-2896	
		CNNVD-202206-2897	
	CNNVD-202206-2898		
	TRENDnet	CNNVD-202206-1664	
	个人开发者	CNNVD-202206-334	
CNNVD-202206-336			
CNNVD-202206-338			
CNNVD-202206-339			

	华为	CNNVD-202206-602	
	吉翁电子	CNNVD-202206-319	
	移远通信	CNNVD-202206-2123	
缓冲区错误	Ascensio System	CNNVD-202206-259	Google Android 缓冲区错误漏洞 (CNNVD-202206-590)
	Blynk	CNNVD-202206-1571	
	Google	CNNVD-202206-507	
		CNNVD-202206-574	
		CNNVD-202206-590	
	H3C	CNNVD-202206-810	
		CNNVD-202206-812	
		CNNVD-202206-813	
		CNNVD-202206-814	
		CNNVD-202206-815	
		CNNVD-202206-817	
		CNNVD-202206-819	
		CNNVD-202206-820	
		CNNVD-202206-821	
		CNNVD-202206-825	
		CNNVD-202206-826	
		CNNVD-202206-827	
		CNNVD-202206-859	
		CNNVD-202206-861	
	CNNVD-202206-862		
	CNNVD-202206-863		
CNNVD-202206-864			
Kakao	CNNVD-202206-1467		
Pyramid Solutions	CNNVD-202206-2245		
Qualcomm	CNNVD-202206-498		
	CNNVD-202206-588		
个人开发者	CNNVD-202206-954		
	CNNVD-202206-2919		
友讯	CNNVD-202206-233		
访问控制错误	Advantech	CNNVD-202206-2724	Siemens SINEMA Remote Connect Server 访问控制错误漏洞 (CNNVD-202206-1253)
	Illumina	CNNVD-202206-384	
	Secheron	CNNVD-202206-2239	
	Siemens	CNNVD-202206-1253	
		CNNVD-202206-1262	
个人开发者	CNNVD-202206-957		
资源管理错误	Eufy	CNNVD-202206-1568	Google Android 资源管理错误漏洞 (CNNVD-202206-587)
	Google	CNNVD-202206-587	
	Qualcomm	CNNVD-202206-499	

	Red Hat	CNNVD-202206-1666	
	Vim	CNNVD-202206-1020	
输入验证错误	Apache 基金会	CNNVD-202206-822	Broadcom CA Automic Automation 输入验证错误漏洞 (CNNVD-202206-1653)
	Broadcom	CNNVD-202206-1653	
		CNNVD-202206-1658	
	Cisco	CNNVD-202206-1532	
	Max Yi	CNNVD-202206-346	
	Mitsubishi Electric	CNNVD-202206-396	
	Qualcomm	CNNVD-202206-711	
	Samsung	CNNVD-202206-719	
		CNNVD-202206-720	
CNNVD-202206-721			
		CNNVD-202206-723	

1. IBM InfoSphere Information Server SQL 注入漏洞

(CNNVD-202206-597)

IBM InfoSphere Information Server 是美国 IBM 公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。

IBM InfoSphere Information Server 11.7 版本存在 SQL 注入漏洞，该漏洞源于易受 SQL 注入攻击。远程攻击者可以发送特制的 SQL 语句，从而允许攻击者查看、添加、修改或删除后端数据库中的信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.ibm.com/support/pages/node/6592573>

2. Laravel 代码问题漏洞 (CNNVD-202206-671)

Laravel 是 Laravel 团队 (Laravel) 的一个 Web 应用程序框架。

Laravel 9.1.8 版本存在安全漏洞，该漏洞源于容易造成远程代码执行。

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://laravel.com/>

3. Siemens SIMATIC WinCC OA 授权问题漏洞 (CNNVD-202206-2079)

Siemens SIMATIC WinCC OA 是德国西门子（Siemens）公司的一个功能强大、灵活多样的 SCADA 操作系统。用于控制和监视工业应用。

Siemens SIMATIC WinCC OA V3.16、V3.17、V3.18 版本存在安全漏洞，该漏洞源于服务器端身份验证 (SSA) 和 Kerberos 身份验证均未启用时，应用程序仅使用客户端身份验证。攻击者利用该漏洞可以冒充其他用户或在未经身份验证的情况下利用客户端-服务器协议。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://cert-portal.siemens.com/productcert/pdf/ssa-111512.pdf>

4. TRENDnet TEW-831DR 操作系统命令注入漏洞 (CNNVD-202206-1664)

TRENDnet TEW-831DR 是美国趋势网络（TRENDnet）公司的一款路由器。

TRENDnet TEW-831DR 1.0 601.130.1.1356 版本存在安全漏洞，该漏洞源于 Web 界面中存在系统命令注入漏洞，允许具有有效凭据的攻击者执行任意 shell 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://research.nccgroup.com/2022/06/10/technical-advisory-multiple-vulnerabilities-in-trendnet-tew-831dr-wifi-router-cve-2022-30325-cve-2022-30326-cve-2022-30327-cve-2022-30328-cve-2022-30329/>

5. Google Android 缓冲区错误漏洞（CNNVD-202206-590）

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。

Google Android 10、11、12、12L 及之前版本中的 Media Framework 存在缓冲区错误漏洞，攻击者利用该漏洞可以远程执行代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://source.android.com/security/bulletin/2022-06-01>

6. Siemens SINEMA Remote Connect Server 访问控制错误漏洞（CNNVD-202206-1253）

Siemens SINEMA Remote Connect Server 是德国西门子（Siemens）公司的一套远程网络管理平台。该平台主要用于远程访问、维护、控制和诊断底层网络。

Siemens SINEMA Remote Connect Server 3.1 之前版本存在安全漏洞，该漏洞源于用于更改用户角色和权限的资源缺少身份验证验证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://cert-portal.siemens.com/productcert/pdf/ssa-484086.pdf>

7. Google Android 资源管理错误漏洞（CNNVD-202206-587）

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。

Google Android 10、11、12、12L 及之前版本存在资源管理错误漏洞，该漏洞源于系统组件中的存在严重安全漏洞，攻击者利用该漏洞可以提升本地权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://source.android.com/security/bulletin/2022-06-01>

8. Broadcom CA Automic Automation 输入验证错误漏洞 (CNNVD-202206-1653)

Broadcom CA Automic Automation 是美国博通（Broadcom）公司的一种自动化产品。提供服务编排和自动化平台，以自动化复杂的应用程序、平台和技术环境。

Broadcom CA Automic Automation 12.2 版本和 12.3 版本存在安全漏洞，该漏洞源于存在输入验证不足问题。远程攻击者通过该漏洞可以执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/20629>

1.4.2 高危漏洞实例

2022 年 6 月高危漏洞共 865 个，其中重要漏洞实例如表 6 所示。

表 6 2022 年 6 月高危漏洞实例

漏洞类型	厂商	CNNVD 编号	漏洞实例	
SQL 注入	Amodat	CNNVD-202206-1170	WordPress plugin amtyThumb SQL 注入漏洞 (CNNVD-202206-796)	
	Brandbugle	CNNVD-202206-733		
	Eatan	CNNVD-202206-731		
	Everywhere	CNNVD-202206-732		
	MINMAX	CNNVD-202206-734		
	MV Informática	CNNVD-202206-243		
	Navetti	CNNVD-202206-1075		
	Prestashop	CNNVD-202206-2672		
	SevOne	CNNVD-202206-740		
	SialWeb	CNNVD-202206-777		
	Simplessus	CNNVD-202206-2776		
	Virtua	CNNVD-202206-669		
	Wolters Kluwer	CNNVD-202206-605		
	WordPress 基金会			CNNVD-202206-796
				CNNVD-202206-1092
				CNNVD-202206-1164
	ZZCMS			CNNVD-202206-1690
				CNNVD-202206-1691
				CNNVD-202206-1692
				CNNVD-202206-1693
				CNNVD-202206-1694
				CNNVD-202206-1698
				CNNVD-202206-1699
	phplist			CNNVD-202206-1707
				CNNVD-202206-1000
	个人开发者			CNNVD-202206-122
				CNNVD-202206-140
				CNNVD-202206-141
				CNNVD-202206-143
				CNNVD-202206-144
		CNNVD-202206-145		
		CNNVD-202206-146		
		CNNVD-202206-147		
		CNNVD-202206-150		
		CNNVD-202206-152		
		CNNVD-202206-153		
		CNNVD-202206-154		
		CNNVD-202206-155		
		CNNVD-202206-156		
	CNNVD-202206-160			
	CNNVD-202206-164			
	CNNVD-202206-166			

		CNNVD-202206-167	
		CNNVD-202206-195	
		CNNVD-202206-203	
		CNNVD-202206-204	
		CNNVD-202206-205	
		CNNVD-202206-206	
		CNNVD-202206-207	
		CNNVD-202206-208	
		CNNVD-202206-209	
		CNNVD-202206-210	
		CNNVD-202206-211	
		CNNVD-202206-212	
		CNNVD-202206-213	
		CNNVD-202206-215	
		CNNVD-202206-216	
		CNNVD-202206-220	
		CNNVD-202206-230	
		CNNVD-202206-231	
		CNNVD-202206-232	
		CNNVD-202206-235	
		CNNVD-202206-354	
		CNNVD-202206-355	
		CNNVD-202206-356	
		CNNVD-202206-357	
		CNNVD-202206-358	
		CNNVD-202206-359	
		CNNVD-202206-360	
		CNNVD-202206-361	
		CNNVD-202206-363	
		CNNVD-202206-364	
		CNNVD-202206-365	
		CNNVD-202206-366	
		CNNVD-202206-367	
		CNNVD-202206-368	
		CNNVD-202206-369	
		CNNVD-202206-370	
		CNNVD-202206-371	
		CNNVD-202206-372	
		CNNVD-202206-373	
		CNNVD-202206-375	
		CNNVD-202206-378	
		CNNVD-202206-380	
		CNNVD-202206-382	

		CNNVD-202206-640	
		CNNVD-202206-775	
		CNNVD-202206-840	
		CNNVD-202206-900	
		CNNVD-202206-944	
		CNNVD-202206-945	
		CNNVD-202206-1325	
		CNNVD-202206-1326	
		CNNVD-202206-1327	
		CNNVD-202206-1331	
		CNNVD-202206-1334	
		CNNVD-202206-1338	
		CNNVD-202206-1342	
		CNNVD-202206-1345	
		CNNVD-202206-1346	
		CNNVD-202206-1348	
		CNNVD-202206-1352	
		CNNVD-202206-1354	
		CNNVD-202206-1357	
		CNNVD-202206-1359	
		CNNVD-202206-1363	
		CNNVD-202206-1365	
		CNNVD-202206-1368	
		CNNVD-202206-1369	
		CNNVD-202206-1372	
		CNNVD-202206-1374	
		CNNVD-202206-1400	
		CNNVD-202206-1402	
		CNNVD-202206-1405	
		CNNVD-202206-1407	
		CNNVD-202206-1416	
		CNNVD-202206-1418	
		CNNVD-202206-1420	
		CNNVD-202206-1423	
		CNNVD-202206-1429	
		CNNVD-202206-1430	
		CNNVD-202206-1434	
		CNNVD-202206-1470	
		CNNVD-202206-1478	
		CNNVD-202206-1479	
		CNNVD-202206-1480	
		CNNVD-202206-1482	
		CNNVD-202206-1483	

		CNNVD-202206-1512	
		CNNVD-202206-1513	
		CNNVD-202206-1514	
		CNNVD-202206-1515	
		CNNVD-202206-1516	
		CNNVD-202206-1517	
		CNNVD-202206-1520	
		CNNVD-202206-1545	
		CNNVD-202206-1547	
		CNNVD-202206-1548	
		CNNVD-202206-1561	
		CNNVD-202206-1562	
		CNNVD-202206-1563	
		CNNVD-202206-1591	
		CNNVD-202206-1592	
		CNNVD-202206-1594	
		CNNVD-202206-1624	
		CNNVD-202206-2131	
		CNNVD-202206-2133	
		CNNVD-202206-2134	
		CNNVD-202206-2141	
		CNNVD-202206-2250	
		CNNVD-202206-2292	
		CNNVD-202206-2293	
		CNNVD-202206-2429	
		CNNVD-202206-2430	
		CNNVD-202206-2431	
		CNNVD-202206-2432	
		CNNVD-202206-2433	
		CNNVD-202206-2434	
		CNNVD-202206-2435	
		CNNVD-202206-2436	
		CNNVD-202206-2437	
		CNNVD-202206-2438	
		CNNVD-202206-2439	
		CNNVD-202206-2440	
		CNNVD-202206-2441	
		CNNVD-202206-2443	
		CNNVD-202206-2445	
		CNNVD-202206-2815	
	迅易科技	CNNVD-202206-2253	
		CNNVD-202206-2255	
		CNNVD-202206-2256	

		CNNVD-202206-2257	
		CNNVD-202206-2258	
		CNNVD-202206-2264	
代码问题	ACEware Systems	CNNVD-202206-299	McAfee Consumer Product Removal Tool 代码问题漏洞 (CNNVD-202206-2043)
	Apache Friends	CNNVD-202206-966	
	Archer	CNNVD-202206-341	
	AutomationDirect	CNNVD-202206-1618	
	DNN	CNNVD-202206-331	
	Dell	CNNVD-202206-1034	
	Docebo	CNNVD-202206-2299	
	Embedthis Software	CNNVD-202206-343	
	Imagemagick Studio	CNNVD-202206-1625	
	McAfee	CNNVD-202206-2043	
		CNNVD-202206-2044	
	Microsoft	CNNVD-202206-1215	
		CNNVD-202206-1366	
	Naver	CNNVD-202206-1163	
	Netscout	CNNVD-202206-404	
	OBDA systems	CNNVD-202206-2144	
	OFFIS	CNNVD-202206-2309	
	SAP	CNNVD-202206-1388	
	Samast Technologies	CNNVD-202206-1233	
	Samsung	CNNVD-202206-677	
	Siemens	CNNVD-202206-1273	
	TYPO3	CNNVD-202206-1287	
	WordPress 基金会	CNNVD-202206-1132	
		CNNVD-202206-2031	
	ZEIT	CNNVD-202206-2661	
	Zoom	CNNVD-202206-1555	
	jrsoftware	CNNVD-202206-1579	
	个人开发者	CNNVD-202206-214	
CNNVD-202206-217			
CNNVD-202206-218			
CNNVD-202206-219			
CNNVD-202206-266			
CNNVD-202206-270			
CNNVD-202206-278			
CNNVD-202206-607			
CNNVD-202206-1148			
CNNVD-202206-1151			
CNNVD-202206-1510			
CNNVD-202206-1578			
CNNVD-202206-1676			

		CNNVD-202206-2022		
授权问题	Adobe	CNNVD-202206-1546	Schneider Electric Wiser Smart 授权问题漏洞 (CNNVD-202206-419)	
	Barco	CNNVD-202206-294		
	BitTorrent	CNNVD-202206-1712		
	Couchbase	CNNVD-202206-1197		
	Dell	CNNVD-202206-416		
	GE	CNNVD-202206-1687		
	GitLab	CNNVD-202206-138		
	Google	CNNVD-202206-593		
	Grafana	CNNVD-202206-1734		
	Hitachi	CNNVD-202206-765		
	Johnson Controls	CNNVD-202206-1458		
	OPC	CNNVD-202206-1607		
	Owl Labs	CNNVD-202206-437		
	Samsung	CNNVD-202206-672		
	Schneider Electric	CNNVD-202206-419		
	个人开发者			CNNVD-202206-251
		CNNVD-202206-1717		
友讯	CNNVD-202206-1648			
操作系统命令注入	Apache 基金会	CNNVD-202206-1471	Tenable Network Security Nessus 操作系统命令注入漏洞 (CNNVD-202206-1599)	
	Carrier	CNNVD-202206-440		
	Dell	CNNVD-202206-413		
	KDDI	CNNVD-202206-2821		
	Poly			CNNVD-202206-660
				CNNVD-202206-661
	SerComm	CNNVD-202206-314		
	Tenable Network Security	CNNVD-202206-1599		
	lifion	CNNVD-202206-340		
	个人开发者			CNNVD-202206-335
		CNNVD-202206-337		
		CNNVD-202206-933		
腾达	CNNVD-202206-249			
缓冲区错误	3S-Smart Software Solutions	CNNVD-202206-2446	Schneider Electric IGSS Data Server 缓冲区错误漏洞 (CNNVD-202206-2004)	
	Adobe			CNNVD-202206-1142
				CNNVD-202206-1145
				CNNVD-202206-1146
				CNNVD-202206-1335
				CNNVD-202206-1340
				CNNVD-202206-1343
				CNNVD-202206-1344
				CNNVD-202206-1349
	CNNVD-202206-1353			

		CNNVD-202206-1358	
		CNNVD-202206-1361	
		CNNVD-202206-1364	
		CNNVD-202206-1377	
		CNNVD-202206-1389	
		CNNVD-202206-1393	
		CNNVD-202206-1396	
		CNNVD-202206-1398	
		CNNVD-202206-1401	
		CNNVD-202206-1403	
		CNNVD-202206-1408	
		CNNVD-202206-1412	
		CNNVD-202206-1413	
		CNNVD-202206-1417	
		CNNVD-202206-1419	
		CNNVD-202206-1422	
		CNNVD-202206-1425	
		CNNVD-202206-1427	
		CNNVD-202206-1437	
		CNNVD-202206-1439	
		CNNVD-202206-1441	
		CNNVD-202206-1442	
		CNNVD-202206-1447	
		CNNVD-202206-1451	
		CNNVD-202206-1452	
	Autodesk	CNNVD-202206-1619	
		CNNVD-202206-1620	
		CNNVD-202206-2120	
		CNNVD-202206-2121	
	Bandisoft	CNNVD-202206-345	
	BitTorrent	CNNVD-202206-1722	
	Dell	CNNVD-202206-118	
	FFmpeg	CNNVD-202206-1737	
		CNNVD-202206-1739	
		CNNVD-202206-1986	
		CNNVD-202206-1990	
	Google	CNNVD-202206-504	
		CNNVD-202206-565	
		CNNVD-202206-589	
		CNNVD-202206-595	
		CNNVD-202206-950	
	JerryScript	CNNVD-202206-2069	
	Mozilla 基金会	CNNVD-202206-2680	

		CNNVD-202206-2682
	NHI	CNNVD-202206-2020
	NVIDIA	CNNVD-202206-867
		CNNVD-202206-871
	Qualcomm	CNNVD-202206-496
		CNNVD-202206-500
		CNNVD-202206-502
		CNNVD-202206-503
		CNNVD-202206-591
		CNNVD-202206-699
	Schneider Electric	CNNVD-202206-2004
		CNNVD-202206-2005
		CNNVD-202206-2006
		CNNVD-202206-2008
		CNNVD-202206-2009
		CNNVD-202206-2010
		CNNVD-202206-2012
	CNNVD-202206-2014	
	Siemens	CNNVD-202206-1258
	Sricam	CNNVD-202206-774
		CNNVD-202206-776
	Vim	CNNVD-202206-947
		CNNVD-202206-1994
		CNNVD-202206-1997
		CNNVD-202206-2058
		CNNVD-202206-2307
		CNNVD-202206-2549
	个人开发者	CNNVD-202206-151
		CNNVD-202206-286
		CNNVD-202206-320
		CNNVD-202206-323
		CNNVD-202206-326
		CNNVD-202206-330
		CNNVD-202206-446
		CNNVD-202206-858
		CNNVD-202206-1200
		CNNVD-202206-2233
		CNNVD-202206-2236
		CNNVD-202206-2263
		CNNVD-202206-2266
	CNNVD-202206-2268	
	CNNVD-202206-2269	
	华为	CNNVD-202206-481

	小米	CNNVD-202206-828	
访问控制错误	Elcomplus LLC	CNNVD-202206-2301	Emerson DeltaV Distributed Control System 访问控制错误漏洞 (CNNVD-202206-2922)
	Emerson	CNNVD-202206-2922	
	GitLab	CNNVD-202206-132	
	Google	CNNVD-202206-1178	
	Gradle	CNNVD-202206-612	
	Hillrom	CNNVD-202206-1651	
	JTEKT	CNNVD-202206-2138	
	Meridian Cooperative	CNNVD-202206-1449	
	Motorola Solutions	CNNVD-202206-2677	
	Schneider Electric	CNNVD-202206-2007	
	Splunk	CNNVD-202206-1485	
资源管理错误	Adobe	CNNVD-202206-1333	Google Android 资源管理错误漏洞 (CNNVD-202206-509)
		CNNVD-202206-1356	
		CNNVD-202206-1378	
		CNNVD-202206-1381	
		CNNVD-202206-1392	
		CNNVD-202206-1433	
	CNNVD-202206-1440		
	Apache 基金会	CNNVD-202206-811	
	Autodesk	CNNVD-202206-2122	
		CNNVD-202206-2124	
	AutomationDirect	CNNVD-202206-1637	
	Dell	CNNVD-202206-417	
	Google	CNNVD-202206-509	
		CNNVD-202206-613	
		CNNVD-202206-934	
		CNNVD-202206-955	
	JerryScript	CNNVD-202206-2070	
	Lightbend	CNNVD-202206-353	
	Linux 基金会	CNNVD-202206-309	
		CNNVD-202206-407	
		CNNVD-202206-899	
	Microsoft	CNNVD-202206-1230	
	MinIO	CNNVD-202206-636	
	Mozilla 基金会	CNNVD-202206-2719	
	OPC	CNNVD-202206-1635	
		CNNVD-202206-1636	
	Qualcomm	CNNVD-202206-495	
CNNVD-202206-695			
CNNVD-202206-1277			
SUSE	CNNVD-202206-2150		
Vim	CNNVD-202206-306		

	个人开发者	CNNVD-202206-271	
		CNNVD-202206-321	
		CNNVD-202206-654	
		CNNVD-202206-960	
		CNNVD-202206-1050	
		CNNVD-202206-1617	
		CNNVD-202206-2265	
		CNNVD-202206-2267	
		CNNVD-202206-2270	
输入验证错误	Adobe	CNNVD-202206-1386	Schneider Electric PowerLogic ION Setup 输入验证错误漏洞 (CNNVD-202206-432)
		CNNVD-202206-1406	
	Apache 基金会	CNNVD-202206-844	
	BigBlueButton 社区	CNNVD-202206-129	
	Dell	CNNVD-202206-2310	
		CNNVD-202206-2314	
		CNNVD-202206-2315	
	Dominion Voting Systems	CNNVD-202206-486	
	Google	CNNVD-202206-531	
		CNNVD-202206-555	
		CNNVD-202206-581	
	Imagemagick Studio	CNNVD-202206-1626	
		CNNVD-202206-1627	
	Microsoft	CNNVD-202206-948	
	Robustel	CNNVD-202206-2901	
	Schneider Electric	CNNVD-202206-432	
Siemens	CNNVD-202206-1250		
个人开发者	CNNVD-202206-1202		
华为	CNNVD-202206-108		
	CNNVD-202206-473		
	CNNVD-202206-598		
	CNNVD-202206-2013		

1. WordPress plugin amtyThumb SQL 注入漏洞

(CNNVD-202206-796)

WordPress 和 WordPress plugin 都是 WordPress 基金会的产品。

WordPress 是一套使用 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 plugin 是一个应用插件。

WordPress plugin amtyThumb 4.2.0 及其之前版本存在 SQL 注入漏洞，该漏洞源于应用不会对短代码使用的参数进行清理转义。经过身份验证的用户可以利用该漏洞进行 SQL 注入攻击。

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/359d145b-c365-4e7c-a12e-c26b7b8617ce>

2. McAfee Consumer Product Removal Tool 代码问题漏洞 (CNNVD-202206-2043)

McAfee Consumer Product Removal Tool 是美国 McAfee 公司的旨在完全删除 McAfee Security 产品以重新安装或安装不同的防病毒软件。

McAfee Consumer Product Removal Tool 10.4.128 之前的版本存在代码问题漏洞，该漏洞源于之前的一个不受控制的搜索路径漏洞可能允许本地攻击者使用特定文件名执行旁加载攻击，这可能导致用户获得提升的权限并能够执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://service.mcafee.com/?articleId=TS103318&page=shell&shell=article-view>

3. Schneider Electric Wiser Smart 授权问题漏洞 (CNNVD-202206-419)

Schneider Electric Wiser Smart 是法国施耐德电气（Schneider Electric）公司的一个完整的互联家庭解决方案。可为家庭带来舒适、便利和安全。

Schneider Electric Wiser Smart 存在授权问题漏洞，该漏洞源于不正确的身份验证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.se.com/ww/en/download/document/SEVD-2022-130-03/>

4. Tenable Network Security Nessus 操作系统命令注入漏洞 (CNNVD-202206-1599)

Tenable Network Security Nessus 是美国 Tenable Network Security 公司的一款开源的系统漏洞扫描器。

Tenable Network Security Nessus 10.1.3 版本及之前版本存在操作系统命令注入漏洞，经过身份验证的攻击者利用该漏洞可以创建一个审计文件，绕过 PowerShell cmdlet 检查并以管理员权限执行命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.tenable.com/downloads/nessus-agents>

5. Schneider Electric IGSS Data Server 缓冲区错误漏洞 (CNNVD-202206-2004)

Schneider Electric IGSS Data Server 是法国施耐德电气（Schneider Electric）公司的一个交互式图形 Scada 系统的数据服务器。

Schneider Electric IGSS Data Server 15.0.0.22140 之前版本存在缓冲区错误漏洞，该漏洞源于应用存在边界错误。远程攻击者可以利用

该漏洞发送特制的日志数据请求消息、触发内存损坏并在目标系统上执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

http://download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-165-01_IGSS_Security_Notification.pdf

6. Emerson DeltaV Distributed Control System 访问控制错误漏洞（CNNVD-202206-2922）

Emerson DeltaV Distributed Control System 是美国艾默生电气（Emerson）公司的一套自动化分布式控制系统。该系统包括网络安全管理、报警管理、批量控制和变更管理等功能。

Emerson DeltaV Distributed Control System 存在访问控制错误漏洞，该漏洞源于固件升级、即插即用、Hawk 服务、管理、SIS 通信和组播在内的几个协议没有认证。

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://guardian.emerson.com/Login/>

7. Google Android 资源管理错误漏洞（CNNVD-202206-509）

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。

Google Android 存在安全漏洞，该漏洞源于在 WIFI Firmware 中，可能会因释放后重用而导致内存损坏。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://source.android.com/security/bulletin/2022-06-01>

8. Schneider Electric PowerLogic ION Setup 输入验证错误漏洞（CNNVD-202206-432）

Schneider Electric PowerLogic ION Setup 是法国施耐德电气（Schneider Electric）公司的一款免费、用户友好的配置工具。为设置和验证 PowerLogic 仪表和其他设备的设置提供了一个直观的环境。

Schneider Electric 存在输入验证错误漏洞。攻击者利用该漏洞导致潜在的远程代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.se.com/ww/en/download/document/SEVD-2022-130-01/>

二、漏洞平台推送情况

2022 年 6 月漏洞平台推送漏洞 28731 个。

表 7 2022 年 6 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	16776
2	补天平台	11955
推送总计		28731

三、接报漏洞情况

2022 年 6 月接报漏洞 1139 个，其中信息技术产品漏洞（通用型漏洞）339 个，网络信息系统漏洞（事件型漏洞）800 个。

表 8 2022 年 6 月接报漏洞情况表

序号	报送单位	漏洞数量
1	北京天融信网络安全技术有限公司	87
2	杭州安恒信息技术股份有限公司	53
3	北京神州绿盟科技有限公司	25
4	北京长亭科技有限公司	15
5	北京华顺信安科技有限公司	12
6	国防科技大学	12
7	北京数字观星科技有限公司	12
8	天津市兴先道科技有限公司	10
9	北京华胜久安科技有限公司	9
10	北京华云安信息技术有限公司	9
11	北京奇虎科技有限公司	9
12	中兴通讯股份有限公司	8
13	北京威努特技术有限公司	6
14	杭州海康威视数字技术股份有限公司	6
15	个人	4
16	中电信数智科技有限公司	4
17	北京天地和兴科技有限公司	4
18	浪潮电子信息产业股份有限公司	4
19	博智安全科技股份有限公司	4
20	北京中测安华科技有限公司	3
21	北京城市学院	3
22	北京永信至诚科技股份有限公司	3
23	北京机沃科技有限公司	2
24	广州天懋信息系统股份有限公司	2
25	上海上讯信息技术股份有限公司	2
26	北京安帝科技有限公司	2
27	上海斗象信息科技有限公司	2
28	奇安信网神信息技术（北京）股份有限公司	2
29	北京小佑科技有限公司	2
30	长春嘉诚信息技术股份有限公司	2
31	道普信息技术有限公司	1
32	华为技术有限公司	1
33	西南交通大学	1
34	浙江木链物联网科技有限公司	1
35	北京启明星辰信息安全技术有限公司	1
36	四川虹微技术有限公司	1
37	墨菲未来科技(北京)有限公司	1
38	华中科技大学网络空间安全学院	1
39	杭州迪普科技股份有限公司	1

40	内蒙古思沃科技有限公司	1
41	中能融合智慧科技有限公司	1
42	北京微步在线科技有限公司	1
43	国网湖南省电力有限公司湘西供电分公司	1
44	中国科学院软件研究所	1
45	四川荔久信息安全技术有限公司	1
46	山东泽鹿安全技术有限公司	1
47	三六零数字安全科技集团有限公司	1
48	北京长亭未来科技有限公司	1
49	北京国舜科技股份有限公司	1
50	中国联合网络通信集团有限公司软件研究院	1
51	北京金睛云华科技有限公司	1
报送合计		1139

四、重大漏洞通报

4.1 Microsoft Windows Support Diagnostic Tool 安全漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于Microsoft Windows Support Diagnostic Tool安全漏洞（CNNVD-202205-4277、CVE-2022-30190）情况的报送。成功利用此漏洞的攻击者，可在目标主机执行恶意代码。Windows 11、Windows 10、Windows 8、Windows 7、Windows Server 2022、Windows Server 2016、Windows Server 2012、Windows Server 2008、Windows Server version 20H2、Windows Server 2022 等多个系统版本均受此漏洞影响。目前，微软官方发布了临时修补措施缓解漏洞带来的危害，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

Microsoft Windows Support Diagnostic Tool 是美国微软公司 Windows 操作系统内的一个程序，用于排除故障并收集诊断数据以供技术人员分析和解决问题。该漏洞源于 Microsoft Windows Support Diagnostic Tool 中的 URL 协议存在逻辑问题，攻击者可诱使目标主机的应用（如 word）通过 Microsoft Windows Support Diagnostic Tool 中的 URL 协议下载并打开特制的文件，进而在目标主机执行恶意代码。

· 危害影响

成功利用此漏洞的攻击者，可在目标主机执行恶意代码。以下操作系统版本受漏洞影响：

Windows Server 2012 R2 (Server Core installation)

Windows Server 2012 R2

Windows Server 2012 (Server Core installation)

Windows Server 2012

Windows Server 2008 R2 for x64-based Systems Service Pack 1
(Server Core installation)

Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2008 for x64-based Systems Service Pack 2
(Server Core installation)

Windows Server 2008 for x64-based Systems Service Pack 2

Windows Server 2008 for 32-bit Systems Service Pack 2 (Server
Core installation)

Windows Server 2008 for 32-bit Systems Service Pack 2

Windows RT 8.1

Windows 8.1 for x64-based systems

Windows 8.1 for 32-bit systems

Windows 7 for x64-based Systems Service Pack 1

Windows 7 for 32-bit Systems Service Pack 1

Windows Server 2016 (Server Core installation)

Windows Server 2016

Windows 10 Version 1607 for x64-based Systems

Windows 10 Version 1607 for 32-bit Systems

Windows 10 for x64-based Systems

Windows 10 for 32-bit Systems

Windows 10 Version 21H2 for x64-based Systems

Windows 10 Version 21H2 for ARM64-based Systems

Windows 10 Version 21H2 for 32-bit Systems

Windows 11 for ARM64-based Systems

Windows 11 for x64-based Systems

Windows Server, version 20H2 (Server Core Installation)

Windows 10 Version 20H2 for ARM64-based Systems

Windows 10 Version 20H2 for 32-bit Systems

Windows 10 Version 20H2 for x64-based Systems

Windows Server 2022 Azure Edition Core Hotpatch

Windows Server 2022 (Server Core installation)

Windows Server 2022

Windows 10 Version 21H1 for 32-bit Systems

Windows 10 Version 21H1 for ARM64-based Systems

Windows 10 Version 21H1 for x64-based Systems

Windows Server 2019 (Server Core installation)

Windows Server 2019

Windows 10 Version 1809 for ARM64-based Systems

Windows 10 Version 1809 for x64-based Systems

Windows 10 Version 1809 for 32-bit Systems

• 修复建议

目前，微软官方发布了临时修补措施缓解漏洞带来的危害，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://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190>

4.2 微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，共 61 个漏洞。包括多款 Microsoft 产品资源管理错误漏洞（CNNVD-202205-2800、CVE-2022-23267）、Microsoft Visual Studio 安全漏洞（CNNVD-202204-3059、CVE-2022-24513）等多个漏洞。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6月14日，微软发布了2022年6月份安全更新，共61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 Azure Real Time Operating System、Microsoft Windows Defender、Microsoft Windows ALPC、Microsoft Windows File History Service、Microsoft Windows Local Security Authority Subsystem Service等。CNNVD对其危害等级进行了评价，其中高危漏洞29个，中危漏洞32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55个新增漏洞的补丁程序，其中高危漏洞29个，中危漏洞26个。

序号	漏洞名称	CNNVD 编号	CVE 编号	危害 等级	官方链接
1	多款 Microsoft 产品 资源管理错误漏洞	CNNVD- 202205-28 00	CVE-2022 -23267	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23267
2	Microsoft Visual Studio 安全漏洞	CNNVD- 202204-30 59	CVE-2022 -24513	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24513
3	Microsoft Windows 权限许可和访问控 制问题漏洞	CNNVD- 202204-31 14	CVE-2022 -24527	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24527
4	Microsoft .NET Framework 输入验证 错误漏洞	CNNVD- 202204-30 08	CVE-2022 -26832	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26832

5	Microsoft SQL Server 安全漏洞	CNNVD- 202206-13 91	CVE-2022 -29143	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29143
6	Microsoft Azure 安 全漏洞	CNNVD- 202206-12 14	CVE-2022 -29149	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29149
7	Microsoft Windows 安全漏洞	CNNVD- 202206-12 86	CVE-2022 -30140	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30140
8	Microsoft Windows File History Service 安全漏洞	CNNVD- 202206-12 83	CVE-2022 -30142	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30142
9	Microsoft Lightweight Directory Access Protocol 安全漏洞	CNNVD- 202206-12 78	CVE-2022 -30143	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30143
10	Microsoft Lightweight Directory Access Protocol 安全漏洞	CNNVD- 202206-12 64	CVE-2022 -30146	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30146
11	Microsoft Windows Installer 安全漏洞	CNNVD- 202206-12 57	CVE-2022 -30147	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30147
12	Microsoft Lightweight Directory Access Protocol 安全漏洞	CNNVD- 202206-12 39	CVE-2022 -30149	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30149
13	Microsoft Windows Defender 安全漏洞	CNNVD- 202206-12 37	CVE-2022 -30150	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30150
14	Microsoft Windows Ancillary Function Driver for WinSock 安全漏洞	CNNVD- 202206-12 34	CVE-2022 -30151	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30151
15	Microsoft Windows 安全漏洞	CNNVD- 202206-12 30	CVE-2022 -30152	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30152
16	Microsoft Lightweight Directory Access Protocol 安全漏洞	CNNVD- 202206-12 28	CVE-2022 -30153	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30153
17	Microsoft SharePoint 安全漏洞	CNNVD- 202206-13 71	CVE-2022 -30158	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30158

18	Microsoft Windows ALPC 安全漏洞	CNNVD- 202206-12 26	CVE-2022 -30160	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30160
19	Microsoft Lightweight Directory Access Protocol 安全漏洞	CNNVD- 202206-12 25	CVE-2022 -30161	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30161
20	Microsoft Hyper-V 安全漏洞	CNNVD- 202206-12 23	CVE-2022 -30163	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30163
21	Microsoft Windows Kerberos 安全漏洞	CNNVD- 202206-12 22	CVE-2022 -30164	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30164
22	Microsoft Windows Kerberos 安全漏洞	CNNVD- 202206-12 19	CVE-2022 -30165	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30165
23	Microsoft Windows Local Security Authority Subsystem Service 安全漏洞	CNNVD- 202206-12 21	CVE-2022 -30166	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30166
24	Microsoft Excel 安 全漏洞	CNNVD- 202206-13 11	CVE-2022 -30173	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30173
25	Microsoft Office 安 全漏洞	CNNVD- 202206-13 99	CVE-2022 -30174	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30174
26	Microsoft Azure Real Time Operating System 安全漏洞	CNNVD- 202206-14 24	CVE-2022 -30178	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30178
27	多款 Microsoft 产品 安全漏洞	CNNVD- 202206-14 32	CVE-2022 -30188	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30188
28	Microsoft Windows Support Diagnostic Tool 操作系统命令 注入漏洞	CNNVD- 202205-42 77	CVE-2022 -30190	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
29	Microsoft Windows SMBv3 代码问题漏 洞	CNNVD- 202206-12 15	CVE-2022 -32230	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-32230
30	Microsoft Windows Kernel 安全漏洞	CNNVD- 202206-12 29	CVE-2022 -30155	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30155
31	Microsoft Office 安 全漏洞	CNNVD- 202206-13	CVE-2022 -30159	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30159

		50			59
32	Microsoft Windows Kernel 安全漏洞	CNNVD-202206-1224	CVE-2022-30162	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30162
33	Microsoft Office 安全漏洞	CNNVD-202206-1329	CVE-2022-30171	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30171
34	Microsoft Office 安全漏洞	CNNVD-202206-1316	CVE-2022-30172	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30172
35	Microsoft .NET Core 和 Microsoft Visual Studio 安全漏洞	CNNVD-202206-1317	CVE-2022-30184	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30184
36	Microsoft Windows Codecs Library 安全漏洞	CNNVD-202206-1341	CVE-2022-29111	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29111
37	多款 Microsoft 产品 安全漏洞	CNNVD-202206-1438	CVE-2022-29119	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29119
38	Microsoft Windows Container Isolation FS Filter Driver 安全漏洞	CNNVD-202206-1300	CVE-2022-30131	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30131
39	Microsoft Windows Container Manager Service 安全漏洞	CNNVD-202206-1291	CVE-2022-30132	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30132
40	Microsoft Windows Media Foundation 安全漏洞	CNNVD-202206-1290	CVE-2022-30135	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30135
41	Microsoft Windows Network File System 安全漏洞	CNNVD-202206-1289	CVE-2022-30136	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136
42	Microsoft Azure 安全漏洞	CNNVD-202206-1362	CVE-2022-30137	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30137
43	Microsoft Lightweight Directory Access Protocol 安全漏洞	CNNVD-202206-1288	CVE-2022-30139	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30139
44	Microsoft Lightweight Directory Access Protocol 安全漏洞	CNNVD-202206-1285	CVE-2022-30141	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30141
45	Microsoft Windows	CNNVD-	CVE-2022	中危	https://msrc.microsoft.com/update-

	Encrypting File System 安全漏洞	202206-12 70	-30145		guide/vulnerability/CVE-2022-30145
46	Microsoft Windows PowerShell 安全漏洞	CNNVD-202206-12 46	CVE-2022-30148	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30148
47	Microsoft Remote Volume Shadow Copy Service 安全漏洞	CNNVD-202206-12 27	CVE-2022-30154	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30154
48	Microsoft SharePoint 安全漏洞	CNNVD-202206-13 87	CVE-2022-30157	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30157
49	Microsoft Windows Codecs Library 安全漏洞	CNNVD-202206-14 11	CVE-2022-30167	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30167
50	Microsoft Windows App Store 安全漏洞	CNNVD-202206-14 54	CVE-2022-30168	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30168
51	Microsoft Azure Real Time Operating System 安全漏洞	CNNVD-202206-14 21	CVE-2022-30177	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30177
52	Microsoft Azure Real Time Operating System 安全漏洞	CNNVD-202206-14 28	CVE-2022-30179	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30179
53	Microsoft Azure Real Time Operating System 安全漏洞	CNNVD-202206-14 31	CVE-2022-30180	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30180
54	Microsoft Windows 安全漏洞	CNNVD-202206-12 20	CVE-2022-30189	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30189
55	Microsoft Windows Codecs Library 安全漏洞	CNNVD-202206-14 65	CVE-2022-30193	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30193

此次更新共包括 6 个更新漏洞的补丁程序，其中中危漏洞 6 个。

序号	漏洞名称	CNNVD 编号	CVE 编号	危害等级	官方链接
1	Microsoft Windows DCOM Server 安全特征问题漏洞	CNNVD-202106-54 6	CVE-2021-26414	中危	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26414
2	Microsoft Windows Codecs Library 安全漏洞	CNNVD-202206-13 47	CVE-2022-22018	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22018
3	Microsoft Windows	CNNVD-	CVE-2022	中危	https://msrc.microsoft.com/update-

	安全漏洞	202206-13 30	-21166		guide/vulnerability/CVE-2022-211 66
4	Microsoft Windows 安全漏洞	CNNVD- 202206-13 36	CVE-2022 -21123	中危	https://msrc.microsoft.com/update- guide/vulnerability/CVE-2022-211 23
5	Microsoft Windows 安全漏洞	CNNVD- 202206-13 39	CVE-2022 -21125	中危	https://msrc.microsoft.com/update- guide/vulnerability/CVE-2022-211 25
6	Microsoft Windows 安全漏洞	CNNVD- 202206-13 32	CVE-2022 -21127	中危	https://msrc.microsoft.com/update- guide/vulnerability/CVE-2022-211 27

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>