北京师范大学网络信息安全通告

2021 年 12 月报告

北京师范大学信息网络中心

2022 年 1 月

目录

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，2021 年 12 月份新增安全漏洞共 1929 个，从厂商分布来看，NETGEAR 公司产品的漏洞数量最多，共发布 211 个；从漏洞类型来看，缓冲区错误类的漏洞占比最大，达到 11.09%。本月新增漏洞中，超危漏洞 255 个、高危漏洞 814 个、中危漏洞 759 个、低危漏洞 101 个，相应修复率分别为 85.49%、91.89%、93.15%以及 98.02%。合计 1772 个漏洞已有修复补丁发布，本月整体修复率 91.86%。

截至 2021 年 12 月 31 日，CNNVD 采集漏洞总量已达 174664 个。

1.1 漏洞增长概况

2021 年 12 月新增安全漏洞 1929 个，与上月（1628 个）相比增加了 18.49%。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 1806 个。

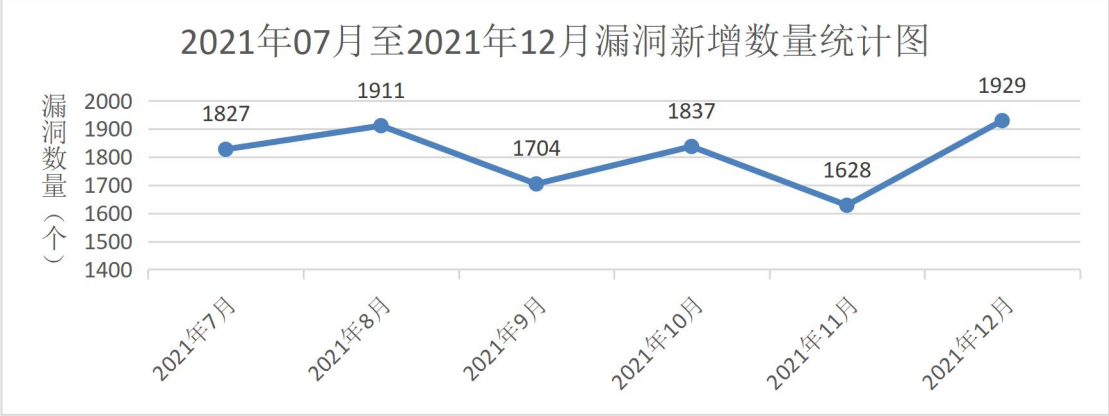

图 1 2021 年 7 月至 2021 年 12 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2021 年 12 月厂商漏洞数量分布情况如表 1 所示，NETGEAR 公司漏洞达到 211 个，占本月漏洞总量的 10.94%。

表 1　2021 年 12 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	NETGEAR	211	10.94%
2	Google	130	6.74%
3	WordPress 基金会	100	5.18%
4	Microsoft	68	3.53%
5	Adobe	64	3.32%
6	Siemens	48	2.49%
7	Mozilla 基金会	40	2.07%
8	IBM	39	2.02%
9	Fortinet	38	1.97%
10	Qualcomm	28	1.45%

1.2.2 漏洞产品分布

2021 年 12 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 38 个，Android 漏洞数量最多，共 104 个，占主流操作系统漏洞总量的 26.80%，排名第一。

表 2　2021 年 12 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	104
2	Windows 10	30
3	Windows Server 2022	29
4	Windows 11	29
5	Windows Server 2019	27

6	Windows Server 2016	22
7	Windows Server 2012	21
8	Windows Server 2012 R2	21
9	Windows 8.1	21
10	Windows Rt 8.1	21
11	Windows 7	19
12	Windows Server 2008	18
13	Windows Server 2008 R2	18
14	Linux Kernel	8

1.2.3 漏洞类型分布

2021 年 12 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 11.09%。

表 3 2021 年 12 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	214	11.09%
2	跨站脚本	213	11.04%
3	代码问题	107	5.55%
4	输入验证错误	79	4.10%
5	信息泄露	75	3.89%
6	SQL 注入	72	3.73%
7	资源管理错误	60	3.11%
8	授权问题	44	2.28%
9	访问控制错误	41	2.13%
10	权限许可和访问控制问题	40	2.07%
11	跨站请求伪造	39	2.02%
12	路径遍历	39	2.02%
13	代码注入	33	1.71%
14	操作系统命令注入	28	1.45%
15	注入	17	0.88%
16	命令注入	17	0.88%
17	加密问题	14	0.73%
18	信任管理问题	13	0.67%
19	竞争条件问题	6	0.31%
20	数据伪造问题	5	0.26%
21	安全特征问题	4	0.21%

22	日志信息泄露	4	0.21%
23	数字错误	4	0.21%
24	环境问题	4	0.21%
25	后置链接	4	0.21%
26	处理逻辑错误	3	0.16%
27	格式化字符串错误	1	0.05%
28	参数注入	1	0.05%
29	其他	748	38.78%

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。12 月漏洞危害等级分布如图 2 所示，其中超危漏洞 255 条，占本月漏洞总数的 13.22%。

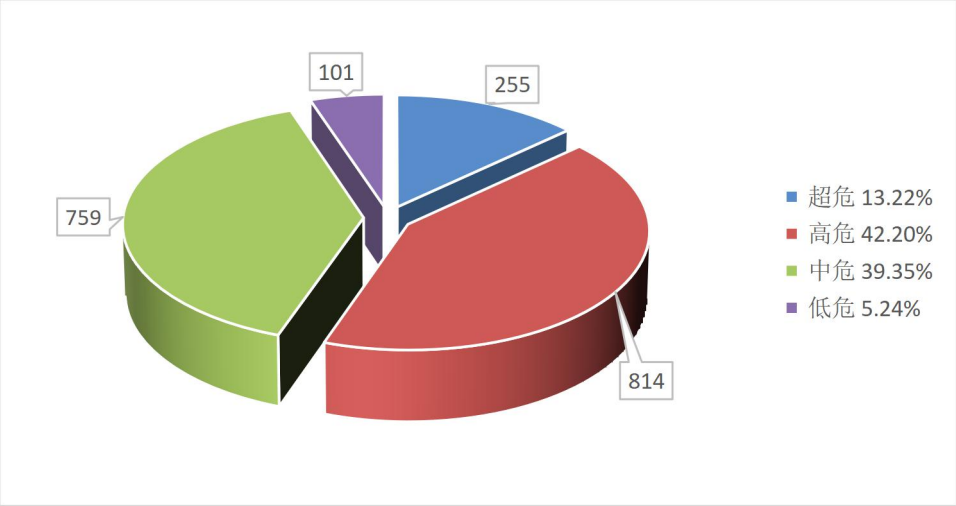

图 2　2021 年 12 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

2021 年 12 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 98.02%，超危漏洞修复率最低，比例为 85.49%。

总体来看，本月整体修复率，由上月的 90.72%上升至本月的 91.86%。

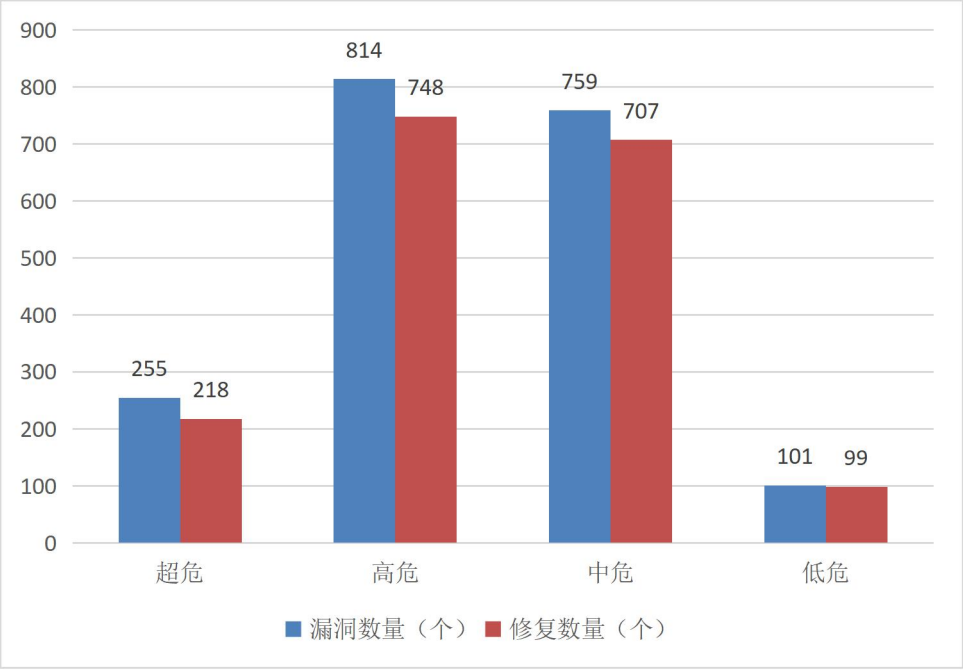

图 3　2021 年 11 月漏洞修复数量统计

1.3.2　厂商修复情况

2021 年 12 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 NETGEAR、Google、WordPress 基金会等十个厂商共 766 条漏洞，占本月漏洞总数的 39.71%，漏洞修复率为 99.48%，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

NETGEAR、Microsoft、Adobe、Siemens、IBM、Fortinet、Qualcomm 等公司本月漏洞修复率均为 100%，共 762 条漏洞已全部修复。

表 4　2021 年 12 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	NETGEAR	211	211	100.00%
2	Google	130	128	98.46%
3	WordPress 基金会	100	99	99.00%
4	Microsoft	68	68	100.00%
5	Adobe	64	64	100.00%
6	Siemens	48	48	100.00%
7	Mozilla 基金会	40	39	97.50%
8	IBM	39	39	100.00%
9	Fortinet	38	38	100.00%
10	Qualcomm	28	28	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

2021 年 12 月超危漏洞共 255 个，其中重要漏洞实例如表 5 所示。

表 5　2021 年 12 月超危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例
SQL注入	Belloo	CNNVD-202112-755	Microsoft Defender SQL 注入漏洞（CNNVD-202112-1167）
	Chamilo协会	CNNVD-202112-204	
	ESRI	CNNVD-202112-445	
	Microsoft	CNNVD-202112-1167	
	PHPGurukul团队	CNNVD-202112-038	
		CNNVD-202112-1043	
	PrestaShop	CNNVD-202112-473	
	Projectworlds	CNNVD-202112-2180	
		CNNVD-202112-2184	
		CNNVD-202112-2185	
		CNNVD-202112-2190	
		CNNVD-202112-2191	
	SAP	CNNVD-202112-1111	
	Tcman	CNNVD-202112-1475	
	WordPress基金会	CNNVD-202112-361	

		CNNVD-202112-366	
		CNNVD-202112-378	
		CNNVD-202112-1033	
		CNNVD-202112-1023	
		CNNVD-202112-1031	
		CNNVD-202112-2102	
	Zzcms团队	CNNVD-202112-1331	
	个人开发者	CNNVD-202112-025	
		CNNVD-202112-072	
		CNNVD-202112-195	
		CNNVD-202112-202	
		CNNVD-202112-203	
		CNNVD-202112-330	
		CNNVD-202112-406	
		CNNVD-202112-768	
		CNNVD-202112-769	
		CNNVD-202112-1242	
		CNNVD-202112-1347	
		CNNVD-202112-1349	
		CNNVD-202112-2111	
		CNNVD-202112-2112	
	顶想信息科技	CNNVD-202112-1372	
代码问题	Adobe	CNNVD-202112-1114	Apache Log4j 代码问题漏洞（CNNVD-202112-799）
	Apache基金会	CNNVD-202112-799	
		CNNVD-202112-1065	
	ChainSea	CNNVD-202112-1574	
	DELL	CNNVD-202112-2122	
	DistributedDataSystems	CNNVD-202112-067	
	MaharashtraStateElectricityDistribution	CNNVD-202112-699	
	NationalLibraryOfTheNetherlands/Research	CNNVD-202112-638	
		CNNVD-202112-639	
	Quest	CNNVD-202112-2162	
		CNNVD-202112-2174	
	RadiantTech	CNNVD-202112-1571	
	SquaredUp	CNNVD-202112-397	
	Veritas	CNNVD-202112-405	
		CNNVD-202112-407	
		CNNVD-202112-408	
		CNNVD-202112-409	
		CNNVD-202112-410	
		CNNVD-202112-413	

	WordPress基金会	CNNVD-202112-1020	
	个人开发者	CNNVD-202112-396	
		CNNVD-202112-824	
		CNNVD-202112-825	
		CNNVD-202112-826	
		CNNVD-202112-829	
		CNNVD-202112-1041	
		CNNVD-202112-1279	
		CNNVD-202112-1334	
		CNNVD-202112-2194	
	顶想信息科技	CNNVD-202112-393	
		CNNVD-202112-395	
授权问题	Belloo	CNNVD-202112-751	Vmware Workspace One Access 授权问题漏洞（CNNVD-202112-1592）
	DistributedDataSystems	CNNVD-202112-077	
	MaharashtraStateElectricityDistribution	CNNVD-202112-478	
	RepriseSoftware	CNNVD-202112-656	
	Siemens	CNNVD-202112-1236	
	Vmware	CNNVD-202112-1592	
	ZOHO	CNNVD-202112-314	
		CNNVD-202112-771	
		CNNVD-202112-1583	
	个人开发者	CNNVD-202112-1246	
		CNNVD-202112-1376	
操作系统命令注入	Lantronix	CNNVD-202112-2192	Lantronix PremierWave 2050 操作系统命令注入漏洞（CNNVD-202112-2192）
	个人开发者	CNNVD-202112-417	
		CNNVD-202112-419	
		CNNVD-202112-2081	
		CNNVD-202112-2082	
		CNNVD-202112-2083	
		CNNVD-202112-2084	
		CNNVD-202112-2085	
		CNNVD-202112-2640	
缓冲区错误	Apache基金会	CNNVD-202112-1579	Apache HTTP Server 缓冲区错误漏洞（CNNVD-202112-1579）
	CIRCUTOR	CNNVD-202112-065	
	D-Link	CNNVD-202112-044	
		CNNVD-202112-045	
		CNNVD-202112-046	
		CNNVD-202112-047	
		CNNVD-202112-048	
		CNNVD-202112-049	
		CNNVD-202112-050	

		CNNVD-202112-051	
	Facebook	CNNVD-202112-477	
	FreeSoftwareFoundation基金会	CNNVD-202112-099	
	Garrett	CNNVD-202112-2074	
	Google	CNNVD-202112-342	
	Lapack社区	CNNVD-202112-725	
	Mozilla基金会	CNNVD-202112-002	
	Sonicwall	CNNVD-202112-557	
	Tenda	CNNVD-202112-196	
	个人开发者	CNNVD-202112-199	
		CNNVD-202112-201	
		CNNVD-202112-728	
		CNNVD-202112-1000	
访问控制错误	BookStackApp	CNNVD-202112-1368	IBM Spectrum Protect Plus 访问控制错误漏洞（CNNVD-202112-787）
	IBM	CNNVD-202112-787	
	个人开发者	CNNVD-202112-1044	
		CNNVD-202112-1237	
		CNNVD-202112-1439	
		CNNVD-202112-1449	
资源管理错误	ARM	CNNVD-202112-1478	ARM mbed TLS 资源管理错误漏洞（CNNVD-202112-1478）
输入验证错误	Fortinet	CNNVD-202112-529	Fortinet FortiOS 输入验证错误漏洞（CNNVD-202112-529）
	Huawei	CNNVD-202112-464	
		CNNVD-202112-465	
	IBM	CNNVD-202112-801	
	个人开发者	CNNVD-202112-325	
		CNNVD-202112-822	
		CNNVD-202112-827	
		CNNVD-202112-1321	

1. Microsoft Defender SQL注入漏洞（CNNVD-202112-1167）

Microsoft Defender是美国微软（Microsoft）公司的一款威胁防护软件。

Microsoft Defender for IoT存在SQL注入漏洞。目前尚无此漏洞的相关信息，请随时关注CNNVD或厂商公告。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42313

2. Lantronix PremierWave 2050 操作系统命令注入漏洞（CNNVD-202112-2192）

Lantronix PremierWave 2050 是美国Lantronix公司的一个嵌入式企业 Wi-Fi 模块。用于提供可靠且始终在线的 5G Wi-Fi 连接。

Lantronix PremierWave 2050 8.9.0.0R4 版本存在安全漏洞，攻击者可以通过特制的HTTP请求导致任意命令执行。

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.lantronix.com/products/premierwave2050/。

3. Apache Log4j 代码问题漏洞（CNNVD-202112-799）

Apache Log4j是美国阿帕奇（Apache）基金会的一款基于Java的开源日志记录工具。

Apache Log4J 存在代码问题漏洞，攻击者可设计一个数据请求发送给使用 Apache Log4j工具的服务器，当该请求被打印成日志时就会触发远程代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://logging.apache.org/log4j/2.x/security.html

4. IBM Spectrum Protect Plus 访问控制错误漏洞（CNNVD-202112-787）

IBM Spectrum Protect Plus是美国IBM公司的一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。

IBM Spectrum Protect Plus存在安全漏洞，该漏洞源于IBM Spectrum Protect Plus使用跨源资源共享(CORS)，但在访问控制头中存在错误配置，它允许攻击者可利用该漏洞执行特权操作并检索敏感信息。

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/6525346

5. Apache HTTP Server 缓冲区错误漏洞（CNNVD-202112-1579）

Apache HTTP Server是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API进行扩充的特点。

Apache HTTP Server 中存在缓冲区错误漏洞，该漏洞源于产品的r:parsebody未能正确判断用户边界。攻击者可通过该漏洞导致缓冲区溢出。以下产品及版本受到影响：Apache HTTP Server 2.4.51 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://httpd.apache.org/download.cgi#apache24

6. Vmware Workspace One Access 授权问题漏洞（CNNVD-202112-1592）

Vmware Workspace One Access是美国Vmware公司的将用户身份与设备和网络信息等因素结合起来，为 Workspace One 交付的应用程序制定智能驱动的条件访问决策。

VMware Workspace ONE Access 21.08, 20.10.0.1, 20.10 版本存在授权问题漏洞，成功提供第一因素身份验证的攻击者可利用该漏洞获得VMware Verify提供的第二因素身份验证。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.vmware.com/security/advisories/VMSA-2021-0030.html

7. Fortinet FortiOS 输入验证错误漏洞（CNNVD-202112-529）

Fortinet FortiOS是美国飞塔（Fortinet）公司的一套专用于FortiGate网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web内容过滤和反垃圾邮件等多种安全功能。

Fortinet FortiOS 存在输入验证错误漏洞，该漏洞可能允许未经身份验证的攻击者通过对 SSLVPN 特制的请求破坏堆上的控制数据，从而导致潜在的任意代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.fortiguard.com/psirt/FG-IR-21-049

8. ARM mbed TLS 资源管理错误漏洞（CNNVD-202112-1478）

ARM mbed TLS是英国ARM公司的一款为mbed产品提供安全通讯和加密功能的产品。

mbed TLS 存在资源管理错误漏洞，远程攻击者可利用该漏洞向应用程序发送一个特别设计的请求来触发一个双重自由错误，并在目标系统上执行任意代码。以下产品及版本受到影响：mbed TLS: 2.0.0, 2.1.0, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 2.1.9, 2.1.10, 2.1.11, 2.1.12, 2.1.13, 2.1.14, 2.1.15, 2.1.16, 2.1.17, 2.1.18, 2.2.0, 2.2.1,

2.3.0, 2.4.0, 2.4.1, 2.4.2, 2.5.0, 2.5.1, 2.6.0, 2.6.1, 2.7.0, 2.7.1, 2.7.2, 2.7.3, 2.7.4, 2.7.5, 2.7.6, 2.7.7, 2.7.8, 2.7.9, 2.7.10, 2.7.11, 2.7.12, 2.7.13, 2.7.14, 2.7.15, 2.7.16, 2.7.17, 2.7.18, 2.7.19, 2.8.0, 2.9.0, 2.10.0, 2.11.0, 2.12.0, 2.13.0, 2.13.1, 2.14.0, 2.14.1, 2.15.0, 2.15.1, 2.16.0, 2.16.1, 2.16.2, 2.16.3, 2.16.4, 2.16.5, 2.16.6, 2.16.7, 2.16.8, 2.16.9, 2.16.10, 2.16.11, 2.17.0, 2.18.0, 2.18.1, 2.19.0, 2.19.1, 2.20.0, 2.21.0, 2.22.0, 2.23.0, 2.24.0, 2.25.0, 2.26.0, 2.27.0, 3.0.0。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tls.mbed.org/tech-updates/security-advisories/mbedtls-security-advisory-2021-12。

1.4.2 高危漏洞实例

2021 年 12 月高危漏洞共 814 个，其中重点漏洞实例如表 6 所示。

表 6　2021 年 12 月高危漏洞实例

漏洞类型	厂商	CNNVD编号	漏洞实例
SQL注入	Amios	CNNVD-202112-2773	SolarWinds Solarwinds Orion SQL注入漏洞（CNNVD-202112-1593）
	DalmarkSystems	CNNVD-202112-2128	
	Fortinet	CNNVD-202112-527	
	Genesys	CNNVD-202112-681	
		CNNVD-202112-682	
	Ivanti	CNNVD-202112-451	
	JFrog	CNNVD-202112-2040	
	Projectworlds	CNNVD-202112-2187	
	Solarwinds	CNNVD-202112-1593	
	SuiteCRM团队	CNNVD-202112-1498	
	Taocms	CNNVD-202112-100	
	WordPress基金会	CNNVD-202112-052	
		CNNVD-202112-1018	
		CNNVD-202112-1022	

		CNNVD-202112-1003	
		CNNVD-202112-2101	
		CNNVD-202112-2108	
	Zzcms团队	CNNVD-202112-750	
		CNNVD-202112-752	
		CNNVD-202112-762	
		CNNVD-202112-763	
	panorama	CNNVD-202112-2758	
	个人开发者	CNNVD-202112-101	
		CNNVD-202112-401	
		CNNVD-202112-516	
		CNNVD-202112-1056	
		CNNVD-202112-1294	
		CNNVD-202112-1362	
		CNNVD-202112-1412	
		CNNVD-202112-1450	
		CNNVD-202112-2161	
代码问题	Apache基金会	CNNVD-202112-1011	Apache HTTP Server 代码问题漏洞（CNNVD-202112-1578）
		CNNVD-202112-1578	
	Autodesk	CNNVD-202112-741	
	Bitdefender	CNNVD-202112-1406	
	Cybonet	CNNVD-202112-706	
	DreamReport	CNNVD-202112-414	
	EmersonElectric	CNNVD-202112-2093	
	FatPipe	CNNVD-202112-687	
	FreeSoftwareFoundation基金会	CNNVD-202112-096	
	GitLab	CNNVD-202112-435	
	Google	CNNVD-202112-243	
		CNNVD-202112-383	
	IBM	CNNVD-202112-788	
	Ivanti	CNNVD-202112-448	
		CNNVD-202112-452	
	JAMF	CNNVD-202112-003	
	Mozilla基金会	CNNVD-202112-547	
	Openssl团队	CNNVD-202112-1132	
	Qualcomm	CNNVD-202112-266	
		CNNVD-202112-269	
		CNNVD-202112-270	
		CNNVD-202112-272	
	Rapid7	CNNVD-202112-1247	
	Sonicwall	CNNVD-202112-597	

	Vmware	CNNVD-202112-1437	
		CNNVD-202112-1591	
	WordPress基金会	CNNVD-202112-2109	
	Z-blog社区	CNNVD-202112-097	
	个人开发者	CNNVD-202112-037	
		CNNVD-202112-198	
		CNNVD-202112-332	
		CNNVD-202112-398	
		CNNVD-202112-823	
		CNNVD-202112-1052	
		CNNVD-202112-1292	
		CNNVD-202112-1320	
		CNNVD-202112-1322	
		CNNVD-202112-1488	
		CNNVD-202112-1489	
		CNNVD-202112-2188	
		CNNVD-202112-2226	
	旭聊科技	CNNVD-202112-006	
授权问题	Apache基金会	CNNVD-202112-2629	Auth0 Express OpenId Connect 授权问题漏洞（CNNVD-202112-754）
	Atlassian	CNNVD-202112-627	
	Auerswald	CNNVD-202112-347	
	Auth0	CNNVD-202112-754	
	BarracudaNetworks	CNNVD-202112-054	
	Django基金会	CNNVD-202112-422	
	Fortinet	CNNVD-202112-734	
	FreseniusKabi	CNNVD-202112-2144	
	Garrett	CNNVD-202112-2072	
	Gryphon	CNNVD-202112-747	
	QNAP	CNNVD-202112-792	
	RepriseSoftware	CNNVD-202112-678	
	Tcman	CNNVD-202112-1476	
	WordPress基金会	CNNVD-202112-2100	
		CNNVD-202112-1272	
	ZOHO	CNNVD-202112-311	
	个人开发者	CNNVD-202112-474	
		CNNVD-202112-764	
		CNNVD-202112-820	
		CNNVD-202112-1329	
		CNNVD-202112-1375	
操作系统命令注入	Abode	CNNVD-202112-1581	Gryphon Tower 操作系统命令注入漏洞
	Elecom	CNNVD-202112-008	

	Fiberhome	CNNVD-202112-1407	（CNNVD-202112-735）
	Gryphon	CNNVD-202112-735	
		CNNVD-202112-738	
		CNNVD-202112-739	
		CNNVD-202112-740	
		CNNVD-202112-742	
		CNNVD-202112-744	
		CNNVD-202112-746	
	Sonicwall	CNNVD-202112-551	
		CNNVD-202112-556	
	TP-Link	CNNVD-202112-2219	
	个人开发者	CNNVD-202112-1588	
缓冲区错误	Adobe	CNNVD-202112-1075	Google Android 缓冲区错误漏洞（CNNVD-202112-363）
		CNNVD-202112-1076	
		CNNVD-202112-1081	
		CNNVD-202112-1086	
		CNNVD-202112-1087	
		CNNVD-202112-1088	
		CNNVD-202112-1095	
		CNNVD-202112-1096	
		CNNVD-202112-1107	
		CNNVD-202112-1110	
		CNNVD-202112-1300	
		CNNVD-202112-1301	
		CNNVD-202112-1302	
		CNNVD-202112-1303	
		CNNVD-202112-1304	
		CNNVD-202112-1305	
		CNNVD-202112-1306	
		CNNVD-202112-1307	
		CNNVD-202112-1309	
		CNNVD-202112-1310	
		CNNVD-202112-1312	
	AllianceForOpenMedia	CNNVD-202112-091	
		CNNVD-202112-093	
	BentleySystems	CNNVD-202112-562	
		CNNVD-202112-563	
		CNNVD-202112-564	
		CNNVD-202112-565	
		CNNVD-202112-566	
		CNNVD-202112-567	

		CNNVD-202112-568	
		CNNVD-202112-569	
		CNNVD-202112-571	
		CNNVD-202112-572	
		CNNVD-202112-581	
		CNNVD-202112-589	
		CNNVD-202112-596	
		CNNVD-202112-612	
		CNNVD-202112-615	
		CNNVD-202112-617	
		CNNVD-202112-618	
		CNNVD-202112-619	
		CNNVD-202112-670	
		CNNVD-202112-671	
		CNNVD-202112-675	
		CNNVD-202112-680	
		CNNVD-202112-686	
		CNNVD-202112-689	
		CNNVD-202112-693	
		CNNVD-202112-698	
		CNNVD-202112-708	
	Codeorigin	CNNVD-202112-1448	
	Fanuc	CNNVD-202112-420	
		CNNVD-202112-421	
	Fortinet	CNNVD-202112-561	
		CNNVD-202112-644	
		CNNVD-202112-701	
		CNNVD-202112-736	
		CNNVD-202112-753	
	GNU社区	CNNVD-202112-1367	
	Garrett	CNNVD-202112-2073	
		CNNVD-202112-2077	
		CNNVD-202112-2078	
	Google	CNNVD-202112-236	
		CNNVD-202112-293	
		CNNVD-202112-301	
		CNNVD-202112-363	
		CNNVD-202112-372	
		CNNVD-202112-384	
		CNNVD-202112-400	
		CNNVD-202112-580	

	IBM	CNNVD-202112-783	
		CNNVD-202112-790	
	Mozilla基金会	CNNVD-202112-721	
	Netgear	CNNVD-202112-2809	
	OpenDesignAlliance	CNNVD-202112-2089	
		CNNVD-202112-2090	
		CNNVD-202112-2107	
	QNAP	CNNVD-202112-781	
	Realtek	CNNVD-202112-2203	
	Rizin组织	CNNVD-202112-1053	
	Siemens	CNNVD-202112-1190	
		CNNVD-202112-1192	
		CNNVD-202112-1193	
		CNNVD-202112-1196	
		CNNVD-202112-1197	
		CNNVD-202112-1204	
		CNNVD-202112-1209	
		CNNVD-202112-1214	
		CNNVD-202112-1216	
		CNNVD-202112-1218	
		CNNVD-202112-1219	
		CNNVD-202112-1220	
		CNNVD-202112-1221	
		CNNVD-202112-1222	
		CNNVD-202112-1224	
		CNNVD-202112-1226	
		CNNVD-202112-1227	
		CNNVD-202112-1231	
		CNNVD-202112-1232	
		CNNVD-202112-1414	
		CNNVD-202112-1419	
	Sonicwall	CNNVD-202112-552	
	WeconTechnologies	CNNVD-202112-731	
	个人开发者	CNNVD-202112-631	
		CNNVD-202112-1120	
		CNNVD-202112-1125	
		CNNVD-202112-1128	
		CNNVD-202112-1129	
		CNNVD-202112-1330	
		CNNVD-202112-1343	
		CNNVD-202112-1480	

		CNNVD-202112-2091	
		CNNVD-202112-2193	
		CNNVD-202112-2266	
		CNNVD-202112-2620	
		CNNVD-202112-2646	
访问控制错误	Elecom	CNNVD-202112-009	Elecom Edwrc 访问控制错误漏洞（CNNVD-202112-009）
	EmersonElectric	CNNVD-202112-2097	
	Fortinet	CNNVD-202112-532	
		CNNVD-202112-634	
	FreseniusKabi	CNNVD-202112-2138	
	Google	CNNVD-202112-1351	
		CNNVD-202112-1352	
	Huawei	CNNVD-202112-460	
	Insulet	CNNVD-202112-031	
	Nvidia	CNNVD-202112-2171	
	PLEX	CNNVD-202112-683	
	Qualcomm	CNNVD-202112-287	
	UniversityofWisconsin-Madison	CNNVD-202112-1400	
	个人开发者	CNNVD-202112-071	
		CNNVD-202112-1440	
	旭聊科技	CNNVD-202112-005	
资源管理错误	BentleySystems	CNNVD-202112-570	Google Chrome 资源管理错误漏洞（CNNVD-202112-348）
		CNNVD-202112-584	
		CNNVD-202112-603	
		CNNVD-202112-674	
		CNNVD-202112-676	
		CNNVD-202112-695	
		CNNVD-202112-702	
		CNNVD-202112-704	
	Fortinet	CNNVD-202112-641	
	FreseniusKabi	CNNVD-202112-2158	
	Google	CNNVD-202112-299	
		CNNVD-202112-300	
		CNNVD-202112-348	
		CNNVD-202112-357	
		CNNVD-202112-364	
		CNNVD-202112-368	
		CNNVD-202112-389	
		CNNVD-202112-411	
		CNNVD-202112-416	
		CNNVD-202112-1051	

		CNNVD-202112-1059	
	Huawei	CNNVD-202112-469	
	IBM	CNNVD-202112-659	
	Linux基金会	CNNVD-202112-2166	
	Microsoft	CNNVD-202112-1153	
		CNNVD-202112-1176	
	Mozilla基金会	CNNVD-202112-544	
		CNNVD-202112-722	
	Qualcomm	CNNVD-202112-291	
		CNNVD-202112-295	
	Siemens	CNNVD-202112-1205	
		CNNVD-202112-1213	
		CNNVD-202112-1228	
	个人开发者	CNNVD-202112-216	
		CNNVD-202112-2225	
输入验证错误	Accops	CNNVD-202112-512	Google Android 输入验证错误漏洞（CNNVD-202112-349）
		CNNVD-202112-513	
		CNNVD-202112-515	
		CNNVD-202112-522	
	Allegro	CNNVD-202112-685	
	Amazon	CNNVD-202112-503	
	AmzettaTechnologies	CNNVD-202112-499	
		CNNVD-202112-501	
	Apache基金会	CNNVD-202112-1577	
	ElectronicTeam	CNNVD-202112-497	
	FlexiHub团队	CNNVD-202112-495	
	Google	CNNVD-202112-268	
		CNNVD-202112-271	
		CNNVD-202112-349	
		CNNVD-202112-1063	
	HornerAutomation	CNNVD-202112-2124	
	Huawei	CNNVD-202112-462	
	NoMachine	CNNVD-202112-481	
		CNNVD-202112-486	
		CNNVD-202112-491	
		CNNVD-202112-485	
	Privoxy团队	CNNVD-202112-794	
		CNNVD-202112-828	
	Qualcomm	CNNVD-202112-256	
		CNNVD-202112-263	
		CNNVD-202112-281	

		CNNVD-202112-289	
	Samsung	CNNVD-202112-648	
		CNNVD-202112-651	
		CNNVD-202112-658	
	StarCharge	CNNVD-202112-2178	
	ZEIT	CNNVD-202112-778	
	个人开发者	CNNVD-202112-490	
		CNNVD-202112-776	
		CNNVD-202112-791	
		CNNVD-202112-1249	
		CNNVD-202112-2780	

1. SolarWinds Solarwinds Orion SQL 注入漏洞（CNNVD-202112-1593）

SolarWinds Solarwinds Orion是SolarWinds公司的一个IT管理产品组合的核心。它提供了一个稳定且可扩展的体系结构，其中包括数据收集，处理，存储和表示。

Solarwinds Orion 存在SQL注入漏洞，具有较低用户权限的攻击者可利用该漏洞窃取密码哈希和密码信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-secure-configuration.htm

2. Gryphon Tower 操作系统命令注入漏洞（CNNVD-202112-735）

Gryphon Tower是Gryphon公司的一款无线路由器。

Gryphon Tower 路由器存在安全漏洞，该漏洞源于/cgi-bin/luci/rc的web界面中的多个参数中存在未经验证的命令注入。攻击者可利用该漏洞通过向web界面发送精心编制的恶意数据包，以root用户身份

在设备上执行命令。

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/security/research/tra-2021-51

3. Apache HTTP Server 代码问题漏洞（CNNVD-202112-1578）

Apache HTTP Server是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的API进行扩充的特点。

Apache HTTP Server 中存在代码问题漏洞，该漏洞源于产品存在空指针引用错误。攻击者可通过该漏洞导致系统奔溃或服务端请求伪造。以下产品及版本受到影响： Apache HTTP Server 2.4.7 至 2.4.51 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://httpd.apache.org/download.cgi#apache24

4. Elecom Edwrc 访问控制错误漏洞（CNNVD-202112-009）

Elecom Edwrc是日本Elecom公司的一系列路由器。

Elecom Edwrc 存在访问控制错误漏洞，该漏洞源于ELECOM路由器未正确限制来自未授权角色的资源访问。

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://jvn.jp/en/vu/JVNVU94527926/index.html

5. Google Android 缓冲区错误漏洞（CNNVD-202112-363）

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

Google Android 11 中的Media Framework 10， 11， 12 之前版本存在缓冲区错误漏洞。该漏洞源于网络系统或产品在运行过程中存在配置等错误。未授权的攻击者可利用漏洞获取受影响组件敏感信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://source.android.com/security/bulletin/2021-12-01

6. Auth0 Express OpenId Connect 授权问题漏洞（CNNVD-202112-754）

Auth0 Express OpenId Connect是美国Auth0 公司的一个开源组件。用于保护 OpenID Connect Web 应用程序的 Express.js 中间件。

Auth0 Express OpenID Connect 存在授权问题漏洞，该漏洞源于不会在用户登录时重新生成会话 ID 和会话 cookie。这种行为使应用程序面临各种会话固定漏洞。

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/auth0/express-openid-connect/security/advisories/GHSA-7rg2-qxmf-hhx9

7. Google Android 输入验证错误漏洞（CNNVD-202112-349）

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

Google Android 11 中的System 9， 10， 11， 12 之前版本存在安全漏洞。

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/2021-12-01

8. Google Chrome 资源管理错误漏洞（CNNVD-202112-348）

Google Chrome是美国谷歌（Google）公司的一款Web浏览器。

Google Chrome 存在资源管理错误漏洞，该漏洞源于在窗口管理器中免费使用后。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2021/12/stable-channel-update-for-desktop.html

二、漏洞平台推送情况

2021 年 12 月漏洞平台推送漏洞 132056 个。

表 7 2021 年 12 月漏洞平台推送情况

序号	漏洞平台	漏洞总量
1	漏洞盒子	97264
2	补天平台	34792
推送总计		132056

三、接报漏洞情况

2021 年 12 月接报漏洞 2399 个，其中信息技术产品漏洞（通用型漏洞）445 个，网络信息系统漏洞（事件型漏洞）1954 个。

表 8 2021 年 12 月漏洞接报情况

序号	报送单位	漏洞总量
1	河南听潮盛世信息技术有限公司	357
2	北京安全共识科技有限公司	311
3	南京众智维信息科技有限公司	254
4	西安四叶草信息技术有限公司	179
5	北京赛宁网安科技有限公司	179
6	北京国舜科技股份有限公司	97
7	北京安帝科技有限公司	87
8	天翼数智科技（北京）有限公司	79
9	北京山石网科信息技术有限公司	71

10	北京数字观星科技有限公司	61
11	杭州海康威视数字技术股份有限公司	51
12	新华三技术有限公司	50
13	北京华云安信息技术有限公司	50
14	北京天融信网络安全技术有限公司	49
15	杭州安恒信息技术股份有限公司	43
16	广州锦行网络科技有限公司	41
17	山东新潮信息技术有限公司	30
18	广州竞远安全技术股份有限公司	24
19	浙江大华技术股份有限公司	24
20	星云博创科技有限公司	22
21	远江盛邦（北京）网络安全科技股份有限公司	20
22	上海上讯信息技术股份有限公司	19
23	浙江宇视科技有限公司	18
24	北京微步在线科技有限公司	15
25	北京鸿腾智能科技有限公司	15
26	北京京东尚科信息技术有限公司	14
27	安徽长泰科技有限公司	14
28	个人	12
29	广州非凡信息安全技术有限公司	12
30	西安交大捷普网络科技有限公司	12
31	国防科技大学	12
32	腾讯科技（北京）有限公司	12
33	北京华夏信安科技有限公司	10
34	北京中测安华科技有限公司	8
35	中国科学院软件研究所、奇安信技术研究院	8
36	信息工程大学	8
37	杭州迪普科技股份有限公司	7
38	四维创智（北京）科技发展有限公司	6
39	百度公司	6
40	北京云测信息技术有限公司	6
41	上海安识网络科技有限公司	6
42	北京神州绿盟科技有限公司	6
43	博智安全科技股份有限公司	6
44	北京梆梆安全科技有限公司	6
45	北京世纪先承信息安全科技有限公司	5
46	上海安几科技有限公司	5
47	国网青海省电力公司电力科学研究院	5
48	山东云天安全技术有限公司	5
49	北京城市学院	4
50	浪潮电子信息产业股份有限公司	4

51	中兴通讯股份有限公司	4
52	北京众安天下科技有限公司	4
53	北京长亭科技有限公司	3
54	北方实验室（沈阳）股份有限公司	3
55	福建经联网络技术有限公司	3
56	北京启明星辰信息安全技术有限公司	3
57	南京赛宁信息技术有限公司	3
58	浙江大学	2
59	中国科学院软件研究所	2
60	北京京宽网络科技有限公司	2
61	北京安天网络安全技术有限公司	2
62	北京聚信得仁科技有限公司	2
63	四川虹微技术有限公司	2
64	南京赛宁网安科技有限公司	2
65	北京机沃科技有限公司	2
66	深圳大学	2
67	北京优炫软件股份有限公司	1
68	北京知道创宇信息技术股份有限公司	1
69	北京容辉智信科技有限公司	1
70	海南神州希望网络有限公司	1
71	上海斗象信息科技有限公司	1
72	南水北调中线信息科技有限公司	1
73	华为技术有限公司	1
74	深圳市深信服电子科技有限公司	1
75	珠海豹趣科技有限公司	1
76	北京智游网安科技有限公司	1
77	恒安嘉新（北京）科技股份公司	1
78	安徽长泰信息安全服务有限公司	1
79	湖南中测网安信息技术有限公司	1
报送合计		**2399**

四、重大漏洞预警

4.1 Apache Log4j 代码问题漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于Apache Log4j代码问题漏洞（CNNVD-202112-799、CVE-2021-44228）情况的报送。成功利用漏洞的攻击者能够在目标服务器上远程执行恶意代码。Apache

Log4j 2.0-2.15.0-rc1 版本受此漏洞影响。目前，Apache官方已发布新版本修复了漏洞，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

Apache Log4j 是 Apache 的一个基于 Java 的日志记录工具，该工具可以控制日志信息输送的目的地为控制台、文件、GUI 组件等，并通过定义每一条日志信息的级别，使其能更加细致地控制日志的生成过程。

由于Apache Log4j中存在JNDI注入漏洞，攻击者可设计一个数据请求发送给使用 Apache Log4j工具的服务器，当该请求被打印成日志时就会触发远程代码执行。

. 危害影响

成功利用漏洞的攻击者能够在目标服务器上远程执行恶意代码。Apache Log4j 2.0-2.15.0-rc1 版本受此漏洞影响。

. 修复建议

目前，Apache 官方已发布新版本修复了漏洞，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://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1

4.2 Apache Apisix 授权问题漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于Apache Apisix 授权问题漏洞（CNNVD-202112-2629、CVE-2021-45232）情况的报送。成功利用漏洞的攻击者，可以在未经授权的情况下获取或更改设备的配置信息，进而构造恶意数据对目标设备进行攻击。Apache APISIX Dashboard 2.10 及其之前版本均受此漏洞影响。目前，Apache官方已经发布了版本更新修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。

. 漏洞介绍

Apache Apisix是美国阿帕奇（Apache）基金会的一个API网关。该网关基于 OpenResty 和 etcd 来实现，具备动态路由和插件热加载等功能，适合微服务体系下的API管理。

Apache Apisix存在授权问题漏洞，攻击者无需登录Apache APISIX Dashboard即可访问某些接口，可在未经授权的情况下更改或获取Apache APISIX相关配置信息，攻击者可利用漏洞构造恶意数据对目标设备进行攻击。

. 危害影响

成功利用漏洞的攻击者，可以在未经授权的情况下获取或更改设备的配置信息，进而构造恶意数据对目标设备进行攻击。Apache APISIX Dashboard 2.10 及其之前版本均受此漏洞影响。

. 修复建议

目前，Apache官方已经发布了版本更新修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。Apache官方更新链接如下：

https://lists.apache.org/thread/979qbl6vlm8269fopfyygnxofgqyn6k5