北京师范大学网络信息安全通告

2022 年 1 月报告

北京师范大学信息网络中心

2022 年 2 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，2022 年 1 月份新增安全漏洞共 2054 个，从厂商分布来看，Oracle 公司产品的漏洞数量最多，共发布 164 个；从漏洞类型来看，输入验证错误类的漏洞占比最大，达到 12.32%。本月新增漏洞中，超危漏洞 234 个、高危漏洞 751 个、中危漏洞 974 个、低危漏洞 95 个，相应修复率分别为 76.92%、87.35%、81.42%以及 98.95%。合计 1723 个漏洞已有修复补丁发布，本月整体修复率 83.89%。

截至 2022 年 01 月 31 日，CNNVD 采集漏洞总量已达 176718 个。

1.1 漏洞增长概况

2022 年 1 月新增安全漏洞 2054 个，与上月（1929 个）相比增加了 6.48%。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 1844 个。

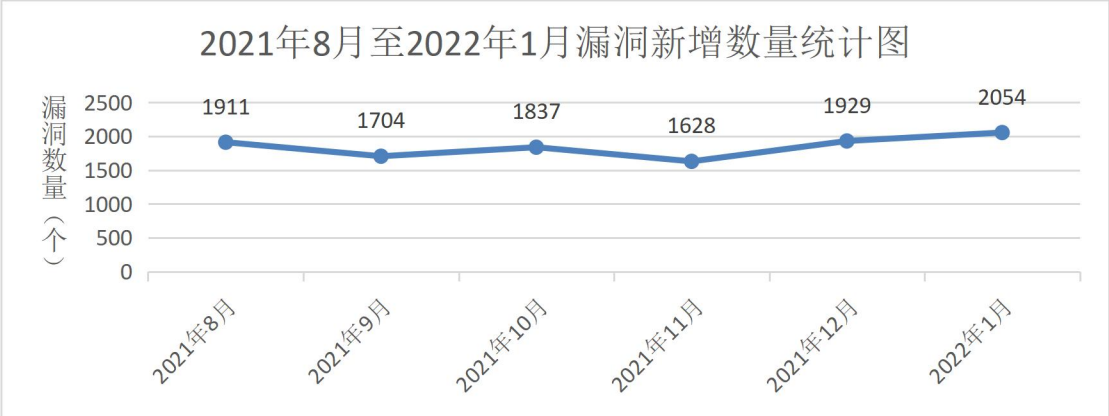

图 1 2021 年 8 月至 2022 年 1 月漏洞新增数量统计图

1.2 漏洞分布情况

1.2.1 漏洞厂商分布

2022 年 1 月厂商漏洞数量分布情况如表 1 所示，Oracle 公司漏洞达到 164 个，占本月漏洞总量的 7.98%。

表 1　2022 年 1 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	Oracle	164	7.98%
2	Microsoft	100	4.87%
3	WordPress 基金会	97	4.72%
4	Google	81	3.94%
5	Adobe	38	1.85%
6	Cisco	30	1.46%
7	Juniper Networks	27	1.31%
8	Huawei	26	1.27%
9	F5	24	1.17%
10	Mozilla 基金会	23	1.12%

1.2.2 漏洞产品分布

2022 年 1 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 85 个，Windows 10 漏洞数量最多，共 78 个，占主流操作系统漏洞总量的 11.29%，排名第一。

表 2　2022 年 1 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	Windows 10	78
2	Windows Server 2019	77
3	Windows Server 2022	76
4	Windows 11	62

5	Windows Server 2016	61
6	Windows Server 2012	52
7	Windows Server 2012 R2	51
8	Windows 8.1	50
9	Windows Rt 8.1	47
10	Windows 7	34
11	Windows Server 2008	34
12	Windows Server 2008 R2	34
13	Android	27

1.2.3 漏洞类型分布

2022 年 1 月份发布的漏洞类型分布如表 3 所示，其中输入验证错误类漏洞所占比例最大，约为 12.32%。

表 3 2022 年 1 月漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	输入验证错误	253	12.32%
2	跨站脚本	231	11.25%
3	缓冲区错误	210	10.22%
4	代码问题	138	6.72%
5	资源管理错误	127	6.18%
6	SQL 注入	90	4.38%
7	信息泄露	58	2.82%
8	权限许可和访问控制问题	50	2.43%
9	跨站请求伪造	39	1.90%
10	授权问题	37	1.80%
11	路径遍历	35	1.70%
12	访问控制错误	32	1.56%
13	安全特征问题	30	1.46%
14	代码注入	26	1.27%
15	命令注入	21	1.02%
16	操作系统命令注入	18	0.88%
17	信任管理问题	18	0.88%
18	注入	13	0.63%
19	加密问题	10	0.49%
20	日志信息泄露	8	0.39%
21	竞争条件问题	6	0.29%
22	环境问题	5	0.24%

23	后置链接	4	0.19%
24	数据伪造问题	3	0.15%
25	数字错误	3	0.15%
26	处理逻辑错误	1	0.05%
27	参数注入	1	0.05%
28	其他	587	28.58%

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 1 月漏洞危害等级分布如图 2 所示，其中超危漏洞 234 条，占本月漏洞总数的 11.39%。

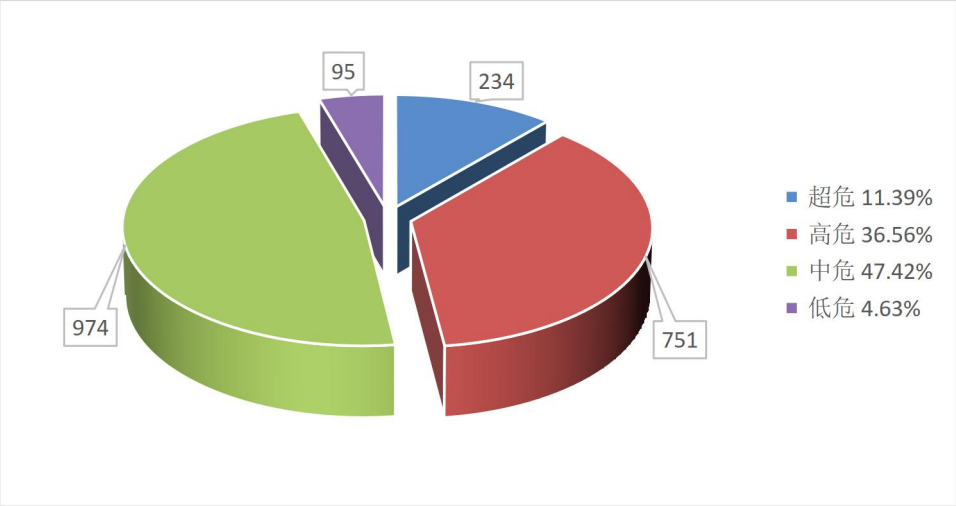

图 2　2022 年 1 月漏洞危害等级分布

1.3 漏洞修复情况

1.3.1 整体修复情况

2022 年 1 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 98.95%，超危漏洞修复率最低，比例为 76.92%。

总体来看，本月整体修复率，由上月的 91.86%下降至本月的 83.89%。

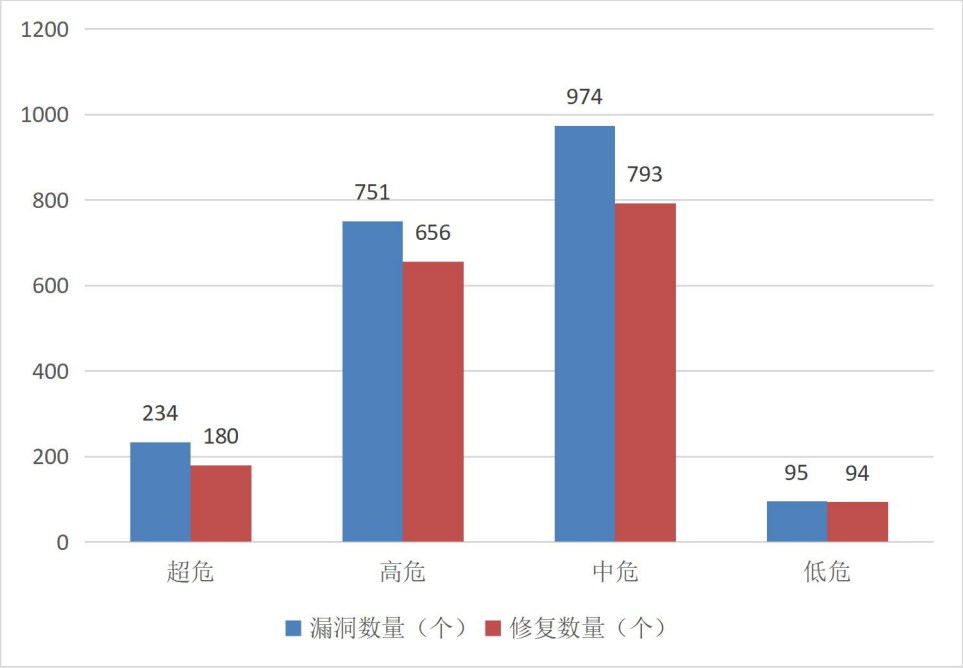

图 3　2022 年 1 月漏洞修复数量统计

1.3.2　厂商修复情况

2022 年 1 月漏洞修复情况按漏洞数量前十厂商进行统计，其中 Oracle、Microsoft、WordPress 基金会等十个厂商共 611 条漏洞，占本月漏洞总数的 29.75%，漏洞修复率为 98.53%，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 Oracle、Adobe、Cisco、Huawei、F5、Mozilla 基金会等公司本月漏洞修复率均为 100%，共 602 条漏洞已全部修复。

表 4　2022 年 1 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	Oracle	164	164	100.00%
2	Microsoft	100	100	100.00%
3	WordPress 基金会	97	95	97.94%
4	Google	81	80	98.77%

5	Adobe	38	38	100.00%
6	Cisco	30	30	100.00%
7	Juniper Networks	27	22	81.48%
8	Huawei	26	26	100.00%
9	F5	24	24	100.00%
10	Mozilla 基金会	23	23	100.00%

1.4 重要漏洞实例

1.4.1 超危漏洞实例

2022 年 1 月超危漏洞共 234 个，其中重要漏洞实例如表 5 所示。

表 5　2022 年 1 月超危漏洞实例

漏洞类型	厂商	CNNVD 编号	漏洞实例
SQL 注入	Apache 基金会	CNNVD-202201-1421	Apache Log4j SQL 注入漏洞（CNNVD-202201-1421）
	ClassApps	CNNVD-202201-2606	
	Elite Graphix	CNNVD-202201-2787	
	H.H.G. Multistore	CNNVD-202201-2647	
		CNNVD-202201-2648	
		CNNVD-202201-2649	
		CNNVD-202201-2657	
	Le-yan	CNNVD-202201-1160	
	MartDevelopers	CNNVD-202201-2300	
	MingSoft	CNNVD-202201-1863	
	Sourcecodester	CNNVD-202201-1815	
		CNNVD-202201-1816	
		CNNVD-202201-1819	
		CNNVD-202201-2140	
		CNNVD-202201-2141	
		CNNVD-202201-2142	
		CNNVD-202201-2143	
		CNNVD-202201-2144	
		CNNVD-202201-2146	
		CNNVD-202201-2154	
		CNNVD-202201-2160	
		CNNVD-202201-2242	
		CNNVD-202201-2243	
		CNNVD-202201-2244	
		CNNVD-202201-2267	

		CNNVD-202201-2593	
		CNNVD-202201-2594	
	WordPress 基金会	CNNVD-202201-653	
		CNNVD-202201-2232	
	个人开发者	CNNVD-202201-183	
		CNNVD-202201-578	
		CNNVD-202201-873	
		CNNVD-202201-877	
		CNNVD-202201-1326	
		CNNVD-202201-1760	
		CNNVD-202201-1813	
		CNNVD-202201-1814	
		CNNVD-202201-2181	
		CNNVD-202201-2182	
		CNNVD-202201-2183	
		CNNVD-202201-2184	
		CNNVD-202201-2191	
		CNNVD-202201-2196	
		CNNVD-202201-2241	
		CNNVD-202201-2245	
		CNNVD-202201-2246	
		CNNVD-202201-2249	
		CNNVD-202201-2251	
		CNNVD-202201-2253	
		CNNVD-202201-2256	
		CNNVD-202201-2315	
		CNNVD-202201-2460	
		CNNVD-202201-2517	
		CNNVD-202201-2518	
		CNNVD-202201-2592	
		CNNVD-202201-2602	
		CNNVD-202201-2771	
代码问题	Apache 基金会	CNNVD-202201-662	Apache Dubbo 代码问题漏洞（CNNVD-202201-662）
		CNNVD-202201-1425	
	Mattermost	CNNVD-202201-1037	
	MingSoft	CNNVD-202201-1855	
		CNNVD-202201-1861	
		CNNVD-202201-2477	
	Schneider Electric	CNNVD-202201-2615	
	Signiant	CNNVD-202201-2708	
	Softvibe	CNNVD-202201-1516	
	Stanford Nlp Group 团队	CNNVD-202201-1390	
	SuiteCRM 团队	CNNVD-202201-2603	

	个人开发者	CNNVD-202201-044	
		CNNVD-202201-186	
		CNNVD-202201-572	
		CNNVD-202201-982	
		CNNVD-202201-1563	
		CNNVD-202201-2316	
		CNNVD-202201-2519	
授权问题	Crestron	CNNVD-202201-1005	ZOHO ManageEngine Desktop Central 授权问题漏洞（CNNVD-202201-1428）
	Dahua	CNNVD-202201-1059	
	IBM	CNNVD-202201-2149	
		CNNVD-202201-2150	
	OpenLens	CNNVD-202201-666	
	Reolink	CNNVD-202201-2347	
	Saviynt	CNNVD-202201-2231	
	Sun & Moon Rise	CNNVD-202201-051	
	Tenda	CNNVD-202201-2607	
	Unisys	CNNVD-202201-2273	
	ZOHO	CNNVD-202201-1428	
	个人开发者	CNNVD-202201-1509	
		CNNVD-202201-1699	
		CNNVD-202201-2250	
操作系统命令注入	China Mobile	CNNVD-202201-1171	Reolink Rlc-410W 操作系统命令注入漏洞（CNNVD-202201-2355）
	Reolink	CNNVD-202201-2352	
		CNNVD-202201-2354	
		CNNVD-202201-2355	
缓冲区错误	Facebook	CNNVD-202201-175	WhatsApp 缓冲区错误漏洞（CNNVD-202201-175）
	Huawei	CNNVD-202201-276	
	QNAP	CNNVD-202201-1147	
		CNNVD-202201-1148	
		CNNVD-202201-1149	
		CNNVD-202201-1150	
		CNNVD-202201-1170	
	Reolink	CNNVD-202201-2487	
	Tp-Link	CNNVD-202201-1387	
	Western Digital	CNNVD-202201-1067	
	个人开发者	CNNVD-202201-009	
		CNNVD-202201-010	
		CNNVD-202201-011	
		CNNVD-202201-012	
		CNNVD-202201-013	
		CNNVD-202201-014	
		CNNVD-202201-018	
		CNNVD-202201-633	

		CNNVD-202201-1750	
		CNNVD-202201-1751	
		CNNVD-202201-2134	
		CNNVD-202201-2492	
		CNNVD-202201-2496	
		CNNVD-202201-2498	
		CNNVD-202201-2595	
		CNNVD-202201-2596	
访问控制错误	Apache 基金会	CNNVD-202201-2308	Apache ShenYu 访问控制错误漏洞（CNNVD-202201-2308）
	Lexmark	CNNVD-202201-1807	
	NUUO	CNNVD-202201-1329	
	个人开发者	CNNVD-202201-181	
资源管理错误	Huawei	CNNVD-202201-080	Huawei Smartphone 资源管理错误漏洞（CNNVD-202201-566）
		CNNVD-202201-566	
	个人开发者	CNNVD-202201-2842	
输入验证错误	Apache 基金会	CNNVD-202201-410	Oracle WebLogic Server 输入验证错误漏洞（CNNVD-202201-1434）
	Huawei	CNNVD-202201-568	
	Lexmark	CNNVD-202201-1805	
	Oracle	CNNVD-202201-1433	
		CNNVD-202201-1434	
		CNNVD-202201-1640	
		CNNVD-202201-1643	
		CNNVD-202201-1644	
	个人开发者	CNNVD-202201-296	
		CNNVD-202201-636	
		CNNVD-202201-637	
		CNNVD-202201-639	
		CNNVD-202201-2194	
		CNNVD-202201-2483	

1. Apache Log4j SQL注入漏洞（CNNVD-202201-1421）

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SQL注入漏洞，该漏洞源于 Log4j 1.2.x 中的 JDBCAppender 接受 SQL 语句作为配置参数，其中要插入的值是来自 PatternLayout 的转换器。 消息转换器 %m 可能总是包含在内。

这允许攻击者通过将精心制作的字符串输入到记录的应用程序的输入字段或标题中来操纵 SQL，从而允许执行意外的 SQL 查询。 请注意，此问题仅在专门配置为使用 JDBCAppender（不是默认设置）时才会影响 Log4j 1.x。 从 2.0-beta8 版本开始，重新引入了 JDBCAppender，适当支持参数化 SQL 查询，并进一步自定义写入日志的列。 Apache Log4j 1.2 已于 2015 年 8 月结束生命周期。用户应升级到 Log4j 2，因为它解决了以前版本中的许多其他问题。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread/pt6lh3pbsvxqlwlp4c5l798dv2hkc85y

2. Reolink Rlc-410W 操作系统命令注入漏洞（CNNVD-202201-2355）

Reolink Rlc-410W是中国Reolink公司的一款 Wifi 安全摄像头。

Reolink RLC-410W v3.0.0.136_20121102 版本的设备网络设置功能存在操作系统命令注入漏洞，一个特别制作的HTTP请求可以导致任意命令的执行。攻击者可以通过发送HTTP请求来触发该漏洞。

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://reolink.com/us/product/rlc-410w/

3. Apache Dubbo 代码问题漏洞（CNNVD-202201-662）

Apache Dubbo是美国阿帕奇（Apache）基金会的一款基于Java的轻量级RPC（远程过程调用）框架。该产品提供了基于接口的远程呼叫、容错和负载平衡以及自动服务注册和发现等功能。

Apache Dubbo hessian-lite 3.2.11 及其早期版本存在代码问题漏

洞，该漏洞源于大多数Dubbo用户使用Hessian2 作为默认的序列化反序列化协议，在Hessian捕获意外异常时，Hessian会为用户注销一些信息，这可能会导致远程执行命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://lists.apache.org/thread/1mszxrvp90y01xob56yp002939c7hlww

4. Apache ShenYu 访问控制错误漏洞（CNNVD-202201-2308）

Apache ShenYu是美国阿帕奇（Apache）基金会的一个异步的，高性能的，跨语言的，响应式的 API 网关。

Apache ShenYu 2.4.0 和 2.4.1 存在访问控制错误漏洞，该漏洞源于用户无需身份验证即可访问 /plugin api。

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/dbrjnnlrf80dr0f92k5r2ysfvf1kr67y

5. WhatsApp 缓冲区错误漏洞（CNNVD-202201-175）

Facebook WhatsApp是美国Facebook公司的一套利用网络传送短信的移动应用程序。该应用程序通过智能手机中的联络人信息，查找使用该软件的联络人传送文字、图片等。

WhatsApp 存在安全漏洞，如果用户对恶意行为者进行 1:1 调用，则 WhatsApp Desktop 可能允许越界写入。以下产品和版本受到影响：WhatsApp for Android prior to v2.21.23, WhatsApp Business for Android prior to v2.21.23, WhatsApp for iOS prior to v2.21.230, WhatsApp Business for iOS prior to v2.21.230, WhatsApp for KaiOS prior to v2.2143, WhatsApp Desktop prior to v2.2146。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.whatsapp.com/security/advisories/2021/

6. ZOHO ManageEngine Desktop Central 授权问题漏洞（CNNVD-202201-1428）

ZOHO ManageEngine Desktop Central（DC）是美国卓豪（ZOHO）公司的一套桌面管理解决方案。该方案包含软件分发、补丁管理、系统配置、远程控制等功能模块，可对桌面机以及服务器管理的整个生命周期提供支持。

ZOHO ManageEngine Desktop Central 存在授权问题漏洞，该漏洞源于允许攻击者绕过身份验证，读取敏感信息或将任意 ZIP 存档上传到服务器。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://pitstop.manageengine.com/portal/en/community/topic/a-critical-security-patch-released-in-desktop-central-and-desktop-central-msp-for-cve-2021-44757-17-1-2022

7. Oracle WebLogic Server 输入验证错误漏洞（CNNVD-202201-1434）

Oracle WebLogic Server是美国甲骨文（Oracle）公司的一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。

Oracle WebLogic Server存在输入验证错误漏洞，该漏洞源于Core

组件中不正确的输入验证。攻击者可利用该漏洞执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.oracle.com/security-alerts/cpujan2022.html

8. Huawei Smartphone 资源管理错误漏洞（CNNVD-202201-566）

Huawei Smartphone是中国华为（Huawei）公司的一款智能手机。

Huawei Smartphone 存在安全漏洞，该漏洞源于智能手机的显示模块存在不受控制的资源消耗漏洞。 成功利用此漏洞可能会影响服务完整性。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://consumer.huawei.com/cn/support/bulletin/2022/1/

1.4.2 高危漏洞实例

2022 年 1 月高危漏洞共 751 个，其中重点漏洞实例如表 6 所示。

表 6　2022 年 1 月高危漏洞实例

漏洞类型	厂商	CNNVD 编号	漏洞实例
SQL 注入	Elite Graphix	CNNVD-202201-2783	Siemens Comos SQL 注入漏洞（CNNVD-202201-864）
		CNNVD-202201-2784	
	MartDevelopers	CNNVD-202201-2302	
	MingSoft	CNNVD-202201-2475	
	Mozilla 基金会	CNNVD-202201-2193	
	Nextcloud	CNNVD-202201-2321	
	Siemens	CNNVD-202201-864	
	Softvibe	CNNVD-202201-1510	
	Sourcecodester	CNNVD-202201-2155	
	Sysaid Technologies	CNNVD-202201-886	
	WordPress 基金会	CNNVD-202201-053	
		CNNVD-202201-067	
		CNNVD-202201-069	
		CNNVD-202201-456	

		CNNVD-202201-461	
		CNNVD-202201-652	
		CNNVD-202201-658	
		CNNVD-202201-2206	
		CNNVD-202201-2207	
		CNNVD-202201-2224	
	ZOHO	CNNVD-202201-677	
	mingSoft	CNNVD-202201-2484	
	pimcore	CNNVD-202201-1411	
	个人开发者	CNNVD-202201-189	
		CNNVD-202201-686	
		CNNVD-202201-1349	
		CNNVD-202201-1778	
		CNNVD-202201-2707	
		CNNVD-202201-2778	
		CNNVD-202201-2782	
代码问题	Acer	CNNVD-202201-2468	Apache Karaf 代码问题漏洞（CNNVD-202201-2285）
	Allwinner Technology	CNNVD-202201-1512	
		CNNVD-202201-1513	
		CNNVD-202201-1690	
	Apache 基金会	CNNVD-202201-412	
		CNNVD-202201-1420	
		CNNVD-202201-2285	
	Bmc Software	CNNVD-202201-400	
	Caldera	CNNVD-202201-990	
	Check Point	CNNVD-202201-561	
	Crater Invoice	CNNVD-202201-978	
		CNNVD-202201-1416	
	F5	CNNVD-202201-1630	
		CNNVD-202201-1635	
		CNNVD-202201-1639	
		CNNVD-202201-1709	
		CNNVD-202201-1712	
		CNNVD-202201-1720	
	GE	CNNVD-202201-2345	
	Google	CNNVD-202201-2462	
	Huawei	CNNVD-202201-289	
		CNNVD-202201-294	
		CNNVD-202201-297	
	IBM	CNNVD-202201-2147	
		CNNVD-202201-2148	
	Jpress 团队	CNNVD-202201-1743	
		CNNVD-202201-2466	

		CNNVD-202201-2471	
	Juniper Networks	CNNVD-202201-902	
		CNNVD-202201-912	
		CNNVD-202201-913	
	Jupyter 社区	CNNVD-202201-2312	
	Leostream	CNNVD-202201-1518	
	Linux 基金会	CNNVD-202201-1165	
	Mattermost	CNNVD-202201-1535	
	Mz Automation	CNNVD-202201-1352	
	Palo Alto Networks	CNNVD-202201-946	
		CNNVD-202201-949	
	PrinterLogic	CNNVD-202201-2774	
	Qualcomm	CNNVD-202201-093	
		CNNVD-202201-099	
	Schneider Electric	CNNVD-202201-2612	
		CNNVD-202201-2616	
	Shopware	CNNVD-202201-304	
	Siemens	CNNVD-202201-869	
	Sourcecodester	CNNVD-202201-432	
		CNNVD-202201-446	
	Stanford Nlp Group 团队	CNNVD-202201-1023	
	Sysaid Technologies	CNNVD-202201-887	
	Unisys	CNNVD-202201-988	
	Western Digital	CNNVD-202201-2632	
	XStream	CNNVD-202201-2709	
	ZOHO	CNNVD-202201-979	
	lib60870	CNNVD-202201-1351	
	pimcore	CNNVD-202201-1526	
	个人开发者	CNNVD-202201-077	
		CNNVD-202201-170	
		CNNVD-202201-608	
		CNNVD-202201-896	
		CNNVD-202201-992	
		CNNVD-202201-1033	
		CNNVD-202201-1327	
		CNNVD-202201-1410	
		CNNVD-202201-1506	
		CNNVD-202201-2162	
		CNNVD-202201-2305	
		CNNVD-202201-2454	
		CNNVD-202201-2515	
		CNNVD-202201-2764	
授权问题	Apache 基金会	CNNVD-202201-892	Western Digital My

	Bottelet	CNNVD-202201-292	Cloud 授权问题漏洞（CNNVD-202201-1068）
	DELL	CNNVD-202201-2174	
	Pegasystems	CNNVD-202201-2619	
	Samsung	CNNVD-202201-627	
	Softvibe	CNNVD-202201-1515	
	Western Digital	CNNVD-202201-1068	
	WordPress 基金会	CNNVD-202201-1403	
	个人开发者	CNNVD-202201-2145	
操作系统命令注入	Cisco	CNNVD-202201-1733	Cisco 多款产品操作系统命令注入漏洞（CNNVD-202201-1733）
	Controlup	CNNVD-202201-157	
	FreeCad 社区	CNNVD-202201-2304	
		CNNVD-202201-2307	
	IBM	CNNVD-202201-1414	
	Jenkins	CNNVD-202201-960	
	Liferay	CNNVD-202201-2645	
		CNNVD-202201-2646	
	Reolink	CNNVD-202201-2349	
		CNNVD-202201-2350	
		CNNVD-202201-2351	
	个人开发者	CNNVD-202201-650	
缓冲区错误	ASUS	CNNVD-202201-048	SonicWall SonicOS 缓冲区错误漏洞（CNNVD-202201-286）
	Adobe	CNNVD-202201-699	
		CNNVD-202201-702	
		CNNVD-202201-707	
		CNNVD-202201-716	
		CNNVD-202201-718	
		CNNVD-202201-720	
		CNNVD-202201-722	
		CNNVD-202201-840	
		CNNVD-202201-846	
		CNNVD-202201-848	
		CNNVD-202201-849	
		CNNVD-202201-852	
		CNNVD-202201-853	
	Allwinner Technology	CNNVD-202201-1508	
	Apple	CNNVD-202201-2404	
		CNNVD-202201-2408	
		CNNVD-202201-2410	
		CNNVD-202201-2416	
		CNNVD-202201-2426	
		CNNVD-202201-2432	
	Autodesk	CNNVD-202201-2198	
		CNNVD-202201-2331	

	Cesanta	CNNVD-202201-2547	
		CNNVD-202201-2551	
		CNNVD-202201-2554	
		CNNVD-202201-2555	
		CNNVD-202201-2557	
		CNNVD-202201-2559	
		CNNVD-202201-2560	
		CNNVD-202201-2564	
	DELL	CNNVD-202201-1641	
	Foxit	CNNVD-202201-2627	
	Freebsd 基金会	CNNVD-202201-856	
	Google	CNNVD-202201-107	
		CNNVD-202201-124	
		CNNVD-202201-125	
		CNNVD-202201-192	
	Huawei	CNNVD-202201-273	
		CNNVD-202201-274	
		CNNVD-202201-278	
		CNNVD-202201-285	
		CNNVD-202201-312	
		CNNVD-202201-567	
	JerryScript	CNNVD-202201-1851	
		CNNVD-202201-1856	
		CNNVD-202201-1858	
		CNNVD-202201-1859	
	Jerryscript	CNNVD-202201-2284	
	Microsoft	CNNVD-202201-733	
		CNNVD-202201-773	
		CNNVD-202201-774	
		CNNVD-202201-775	
		CNNVD-202201-789	
		CNNVD-202201-791	
		CNNVD-202201-801	
		CNNVD-202201-805	
		CNNVD-202201-843	
		CNNVD-202201-854	
	Moddable	CNNVD-202201-1824	
		CNNVD-202201-1827	
		CNNVD-202201-1831	
		CNNVD-202201-1834	
	Mozilla 基金会	CNNVD-202201-046	
		CNNVD-202201-739	
	Omron	CNNVD-202201-427	

	Open Design Alliance	CNNVD-202201-1017	
	Schneider Electric	CNNVD-202201-940	
	SonicWall	CNNVD-202201-286	
		CNNVD-202201-293	
	Vmware	CNNVD-202201-112	
	Xiaomi	CNNVD-202201-1528	
	all3dp	CNNVD-202201-698	
	个人开发者	CNNVD-202201-017	
		CNNVD-202201-021	
		CNNVD-202201-039	
		CNNVD-202201-447	
		CNNVD-202201-575	
		CNNVD-202201-594	
		CNNVD-202201-695	
		CNNVD-202201-697	
		CNNVD-202201-972	
		CNNVD-202201-993	
		CNNVD-202201-1362	
		CNNVD-202201-1787	
		CNNVD-202201-1818	
		CNNVD-202201-1823	
		CNNVD-202201-2190	
		CNNVD-202201-2269	
		CNNVD-202201-2295	
		CNNVD-202201-2311	
		CNNVD-202201-2329	
		CNNVD-202201-2343	
		CNNVD-202201-2480	
		CNNVD-202201-2653	
		CNNVD-202201-2655	
		CNNVD-202201-2713	
		CNNVD-202201-2717	
访问控制错误	Apache 基金会	CNNVD-202201-408	Apache Kylin 访问控制错误漏洞（CNNVD-202201-408）
		CNNVD-202201-2330	
	Bosch	CNNVD-202201-1769	
	F5	CNNVD-202201-1786	
	Lens 团队	CNNVD-202201-2338	
	Reolink	CNNVD-202201-2356	
		CNNVD-202201-2357	
		CNNVD-202201-2359	
		CNNVD-202201-2360	
	WordPress 基金会	CNNVD-202201-2208	
	个人开发者	CNNVD-202201-609	

资源管理错误	Adobe	CNNVD-202201-701	Google Android 资源管理错误漏洞（CNNVD-202201-101）
		CNNVD-202201-712	
		CNNVD-202201-714	
		CNNVD-202201-717	
		CNNVD-202201-719	
		CNNVD-202201-721	
		CNNVD-202201-724	
	Allwinner Technology	CNNVD-202201-1748	
	Apache 基金会	CNNVD-202201-422	
	Apple	CNNVD-202201-2424	
	Cesanta	CNNVD-202201-2561	
	Django 基金会	CNNVD-202201-089	
	F5	CNNVD-202201-1634	
		CNNVD-202201-1705	
		CNNVD-202201-1741	
	Fernhill Software	CNNVD-202201-435	
	Foxit	CNNVD-202201-2628	
	Google	CNNVD-202201-101	
		CNNVD-202201-106	
		CNNVD-202201-115	
		CNNVD-202201-118	
		CNNVD-202201-121	
		CNNVD-202201-131	
		CNNVD-202201-135	
		CNNVD-202201-136	
		CNNVD-202201-139	
		CNNVD-202201-144	
		CNNVD-202201-165	
		CNNVD-202201-1725	
		CNNVD-202201-1730	
		CNNVD-202201-1734	
		CNNVD-202201-1736	
		CNNVD-202201-1739	
		CNNVD-202201-1746	
		CNNVD-202201-1753	
		CNNVD-202201-1764	
		CNNVD-202201-1782	
		CNNVD-202201-1783	
	HDF	CNNVD-202201-2169	
	Huawei	CNNVD-202201-307	
	Juniper Networks	CNNVD-202201-919	
		CNNVD-202201-1075	
		CNNVD-202201-1385	

	Linux 基金会	CNNVD-202201-468	
		CNNVD-202201-1700	
		CNNVD-202201-2463	
		CNNVD-202201-2702	
	Microsoft	CNNVD-202201-858	
		CNNVD-202201-859	
	Mozilla 基金会	CNNVD-202201-747	
	Nvidia	CNNVD-202201-959	
	Qualcomm	CNNVD-202201-100	
	Reolink	CNNVD-202201-2358	
		CNNVD-202201-2476	
	WordPress 基金会	CNNVD-202201-056	
	ZEIT	CNNVD-202201-2656	
	个人开发者	CNNVD-202201-037	
		CNNVD-202201-596	
		CNNVD-202201-601	
		CNNVD-202201-1047	
		CNNVD-202201-1048	
		CNNVD-202201-1054	
		CNNVD-202201-1369	
		CNNVD-202201-1576	
		CNNVD-202201-2715	
输入验证错误	ASUS	CNNVD-202201-2132	Qualcomm 组件输入验证错误漏洞（CNNVD-202201-102）
	Adobe	CNNVD-202201-715	
	Allwinner Technology	CNNVD-202201-1740	
	Apache 基金会	CNNVD-202201-2820	
	Cisco	CNNVD-202201-1729	
	ClamAV	CNNVD-202201-1076	
	DELL	CNNVD-202201-2262	
	F5	CNNVD-202201-1647	
	Google	CNNVD-202201-105	
		CNNVD-202201-108	
	IBM	CNNVD-202201-570	
		CNNVD-202201-2482	
	Linux 基金会	CNNVD-202201-1423	
	MediaTek	CNNVD-202201-164	
	Microsoft	CNNVD-202201-732	
		CNNVD-202201-807	
	Oracle	CNNVD-202201-1422	
		CNNVD-202201-1435	
		CNNVD-202201-1436	
		CNNVD-202201-1588	
		CNNVD-202201-1590	

		CNNVD-202201-1654	
	Pexip	CNNVD-202201-1374	
		CNNVD-202201-1376	
		CNNVD-202201-1377	
		CNNVD-202201-1378	
		CNNVD-202201-1379	
	Qualcomm	CNNVD-202201-102	
	Reolink	CNNVD-202201-2386	
		CNNVD-202201-2397	
		CNNVD-202201-2399	
		CNNVD-202201-2400	
		CNNVD-202201-2401	
		CNNVD-202201-2402	
		CNNVD-202201-2403	
		CNNVD-202201-2406	
		CNNVD-202201-2407	
		CNNVD-202201-2411	
		CNNVD-202201-2413	
		CNNVD-202201-2414	
		CNNVD-202201-2415	
		CNNVD-202201-2417	
		CNNVD-202201-2418	
		CNNVD-202201-2422	
		CNNVD-202201-2425	
		CNNVD-202201-2427	
		CNNVD-202201-2445	
		CNNVD-202201-2447	
		CNNVD-202201-2456	
		CNNVD-202201-2461	
		CNNVD-202201-2494	
		CNNVD-202201-2499	
	Samsung	CNNVD-202201-613	
	Schneider Electric	CNNVD-202201-2618	
		CNNVD-202201-2626	
	Siemens	CNNVD-202201-870	
	个人开发者	CNNVD-202201-417	
		CNNVD-202201-640	
		CNNVD-202201-641	
		CNNVD-202201-643	
		CNNVD-202201-682	
		CNNVD-202201-891	
		CNNVD-202201-1449	

1. Siemens Comos SQL注入漏洞（CNNVD-202201-864）

Siemens Comos是德国西门子（Siemens）公司的一个工厂工程软件解决方案。用于过程工业。

Siemens COMOS Web 存在SQL注入漏洞，该漏洞源于 COMOS 的 COMOS Web 组件易受 SQL 注入攻击。这可能允许攻击者执行任意 SQL 语句。

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-995338.pdf

2. Apache Karaf 代码问题漏洞（CNNVD-202201-2285）

Apache Karaf是美国阿帕奇（Apache）基金会的一款用于部署应用程序和组件的轻量级的OSGi（Java动态化模块化系统）容器。

Apache Karaf 存在代码问题漏洞，该漏洞源于在处理序列化数据时输入验证不安全，远程攻击者可利用该漏洞可以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://issues.apache.org/jira/browse/KARAF-7312

3. Western Digital My Cloud 授权问题漏洞（CNNVD-202201-1068）

Western Digital My Cloud是美国西部数据（Western Digital）公司的一款个人云存储设备。

Western Digital My Cloud OS 5 存在安全漏洞，攻击者可利用该漏洞实现远程代码执行和升级权限。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.westerndigital.com/support/product-security/wdc-22002-my-cloud-os5-firmware-5-19-117

4. Cisco 多款产品操作系统命令注入漏洞（CNNVD-202201-1733）

Cisco Enterprise NFV Infrastructure Software（NFVIS）和Cisco Network Services Orchestrator（NSO）都是美国思科（Cisco）公司的产品。Cisco Enterprise NFV Infrastructure Software是一套NVF基础架构软件平台。该平台可以通过中央协调器和控制器实现虚拟化服务的全生命周期管理。Cisco Network Services Orchestrator是一套网络自动化服务解决方案。

Cisco 多款产品存在操作系统命令注入漏洞，该漏洞源于多个 Cisco 产品的 CLI 实施中的漏洞可能允许经过身份验证的本地攻击者执行命令注入攻击。 此漏洞是由于对受影响产品的过程参数的验证不充分。 攻击者可以通过在此过程执行期间注入命令来利用此漏洞。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cli-cmdinj-4MttWZPB

5. SonicWall SonicOS 缓冲区错误漏洞（CNNVD-202201-286）

Sonicwall SonicWall SonicOS是美国SonicWall（Sonicwall）公司的一套专为SonicWall防火墙设备设计的操作系统。

SonicWall SonicOS存在安全漏洞，该漏洞源于系统处理HTTP Content-Length响应头时出现边界错误而存在的。远程未经身份验证的攻击者可利用该漏洞可以发送专门设计的HTTP响应，触发基于堆栈的缓冲区溢出，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，详情请关注厂商主页：

https://www.sonicwall.com/products/sonicos/

6. Apache Kylin 访问控制错误漏洞（CNNVD-202201-408）

Apache Kylin是美国阿帕奇（Apache）基金会的一款开源的分布式分析型数据仓库。该产品主要提供Hadoop/Spark之上的SQL查询接口及多维分析（OLAP）等功能。

Apache kylin 存在访问控制错误漏洞，该漏洞源于在Apache Kylin中，允许从任何来源发送带有凭据的跨来源请求。

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/rzv4mq58okwj1n88lry82ol2wwm57q1m

7. Google Android 资源管理错误漏洞（CNNVD-202201-101）

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Pixel Telephony 存在安全漏洞，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，详情请关注厂商主页：

https://source.android.com/security/bulletin/pixel/2022-01-01

8. Qualcomm 组件 输入验证错误漏洞（CNNVD-202201-102）

Qualcomm 组件是美国高通（Qualcomm）公司的一个组件。提供高通设备功能的内在部件。

Qualcomm 组件存在安全漏洞，该漏洞源于Hypervisor 中内存区域验证不正确会导致区域映射不正确影响以下产品和版本：AR8031、AR8035、CSRA6620、CSRA6640、CSRB31024、FSM10055、FSM10056、MDM9150、MDM9205、QCA4004、QCA40764、QCA4004、QCA663、QCA663 、 QCA6664CA0 QCA6564 ， QCA6564A ， QCA6564AU ，QCA6574，QCA6574A，QCA6574AU，QCA6595AU，QCA6696，QCA8337，QCA9377，QCA9984，QCM2290，QCM4290，QCM6490，QCS2290，QCS405，QCS410，QCS4290，QCS603，QCS605，QCS610，QCS6490，QCX315，QRB5165，QRB5165N， QSM8250、SA415M、SA515M、SA6145P、SA6150P、SA6155、SA6155P、SA8145P、SA8150P、SA8155、SA8155P、SA8195P、SD 675、SD 8cx Gen2、SD6、SD76、SD66、SD76、SD76、SD76、SD76、SD76、SD76、57G SD750G，SD765，SD765G，SD768G，SD778G，SD7c，SD865 5G，SD870，SD888 5G，SDX24，SDX55，SDX55M，SDX57M，SDXR1，SDXR2 5G，SM6225，SM6250，SM6250P，SM6375，SM7250P，SM7325P，WCD9306，WCD9335，WCD9370 , WCD9375, WCD9380, WCD9385, WCN3910, WCN3950, WCN3988, WCN3991, WCN3999, WCN6750, WCN6850, WCN6851, WCN6855, WCN6856、WSA8830、WSA8835。

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://source.android.com/security/bulletin/pixel/2022-01-01

二、漏洞平台推送情况

2022 年 1 月漏洞平台推送漏洞 36437 个。

表 7 2022 年 1 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	34887
2	补天平台	1550
推送总计		36437

三、接报漏洞情况

2022 年 1 月接报漏洞 3638 个，其中信息技术产品漏洞（通用型漏洞）279 个，网络信息系统漏洞（事件型漏洞）3359 个。

表 8 2022 年 1 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	801
2	西安四叶草信息技术有限公司	562
3	北京国舜科技股份有限公司	497
4	北京山石网科信息技术有限公司	474
5	河南听潮盛世信息技术有限公司	244
6	北京华云安信息技术有限公司	183
7	南京众智维信息科技有限公司	145
8	北京天融信网络安全技术有限公司	74
9	杭州默安科技有限公司	62
10	道普信息技术有限公司	50
11	安徽长泰科技有限公司	39
12	广州易东信息安全技术有限公司	38
13	上海安洵信息技术有限公司	32
14	天翼数智科技（北京）有限公司	30
15	北京数字观星科技有限公司	28
16	山东新潮信息技术有限公司	26
17	杭州海康威视数字技术股份有限公司	26
18	华为技术有限公司	21
19	火线安全	20

20	远江盛邦（北京）网络安全科技股份有限公司	20
21	广州锦行网络科技有限公司	20
22	星云博创科技有限公司	20
23	上海安几科技有限公司	19
24	深圳融安网络科技有限公司	18
25	北京神州绿盟科技有限公司	16
26	广州竞远安全技术股份有限公司	16
27	北京安华金和科技有限公司	15
28	安全邦（北京）信息技术有限公司	14
29	中国电信集团系统集成有限责任公司	10
30	上海上讯信息技术股份有限公司	9
31	北京众安天下科技有限公司	9
32	北京网御星云信息技术有限公司	9
33	浪潮电子信息产业股份有限公司	8
34	北京京东尚科信息技术有限公司	8
35	亚信科技（成都）有限公司	8
36	浙江宇视科技有限公司	8
37	北京汇志凌云数据技术有限责任公司	7
38	北京鸿腾智能科技有限公司	7
39	上海安识网络科技有限公司	6
40	北京华顺信安科技有限公司	5
41	个人	5
42	北京威努特技术有限公司	4
43	战略支援部队信息工程大学	4
44	北京智游网安科技有限公司	4
45	上海斗象信息科技有限公司	2
46	西安交大捷普网络科技有限公司	2
47	四川大学信息安全研究所、上海安般信息科技有限公司	1
48	国防科技大学	1
49	北京世纪先承信息安全科技有限公司	1
50	中国民生银行信用卡中心	1
51	南京赛宁信息技术有限公司	1
52	湖南中测网安信息技术有限公司	1
53	四维创智（北京）科技发展有限公司	1
54	中国科学院信息工程研究所	1
55	杭州安恒信息技术股份有限公司	1
56	北京机沃科技有限公司	1
57	腾讯科技（北京）有限公司	1
58	战吧火星人保护协会	1
59	天津市兴先道科技有限公司	1
报送合计		3638

四、重大漏洞预警

4.1 Apache Log4j 多个安全漏洞的预警

近日，Apache官方发布了多个安全漏洞的公告，包括Apache log4j 代码问题漏洞（CNNVD-202201-1425、CVE-2022-23307）、Apache Log4j SQL注入漏洞（CNNVD-202201-1421、CVE-2022-23305）、Apache log4j 代码问题漏洞（CNNVD-202201-1420、CVE-2022-23302）等。成功利用上述漏洞的攻击者可以在目标系统上执行恶意代码。Apache Log4j 1.x、Apache Chainsaw 2.1.0 之前版本均受漏洞影响。目前，Apache官方已经发布了新版本修复了漏洞，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

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 代码问题漏洞（CNNVD-202201-1425、CVE-2022-23307）：漏洞源于程序处理序列化数据时对输入验证不足导致，攻击者通过将特制数据传递给应用程序，从而执行任意代码。

Apache Log4j SQL注入漏洞（CNNVD-202201-1421、CVE-2022-23305）：漏洞源于程序中的JDBCAppender对用户提供的数据过滤不严格导致，攻击者可利用漏洞向目标系统发送特制请求，进而在应用程序数据库中执行任意SQL命令。

Apache log4j 代码问题漏洞（CNNVD-202201-1420、CVE-2022-23302）：漏洞源于程序处理序列化数据时对输入验证不足导致，攻击者可通过提供一个TopicConnection-FactoryBindingName配置，使程序中的JMSSink执行JNDI请求，进而执行任意代码。

. 危害影响

成功利用上述漏洞的攻击者可以在目标系统上执行恶意代码。Apache Log4j 1.x、Apache Chainsaw 2.1.0 之前版本均受漏洞影响。

. 修复建议

目前，Apache 官方已经发布了新版本修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。Apache 官方补丁下载地址：

https://logging.apache.org/chainsaw/2.x/download.html

4.2 Polkit 安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于Polkit 安全漏洞（CNNVD-202201-2343、CVE-2021-4034）情况的报送。成功利用此漏洞的攻击者，可在默认配置下提升本地用户权限。Polkit 0.92-0.115 版本均受此漏洞影响。目前，Polkit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

Polkit是一个在类 Unix操作系统中控制系统范围权限的组件，通过定义和审核权限规则，实现不同优先级进程间的通讯。Polkit存在于所有主流的Linux发行版的默认配置中，攻击者可通过修改环境变量来利用此漏洞，进而提升本地用户权限。

. 危害影响

成功利用此漏洞的攻击者，可在默认配置下提升本地用户权限。Polkit 0.92-0.115 版本均受此漏洞影响。

. 修复建议

目前，Polkit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/freedesktop/polkit/tags