

信息安全漏洞周报

(2024 年第 1 期 总第 709 期)

信息安全测评中心

2023 年 12 月 31 日

根据国家信息安全漏洞库 (CNNVD) 统计, 本周 (2023 年 12 月 25 日至 2023 年 12 月 31 日) 安全漏洞情况如下:

公开漏洞情况

本周 CNNVD 采集安全漏洞 434 个。

接报漏洞情况

本周 CNNVD 接报漏洞 82120 个, 其中信息技术产品漏洞 (通用型漏洞) 864 个, 网络信息系统漏洞 (事件型漏洞) 497 个, 漏洞平台推送漏洞 80759 个。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，本周新增安全漏洞 434 个，漏洞新增数量有所下降。从厂商分布来看 WordPress 基金会新增漏洞最多，有 127 个；从漏洞类型来看，SQL 注入类的安全漏洞占比最大，达到 16.13%。新增漏洞中，超危漏洞 22 个，高危漏洞 26 个，中危漏洞 382 个，低危漏洞 4 个。

（一）安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 434 个。

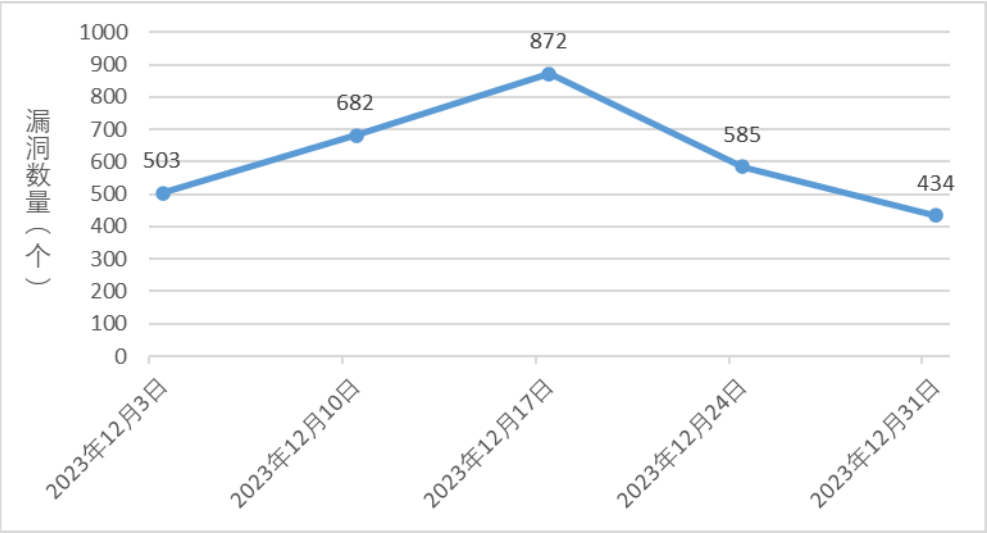


图 1 近五周漏洞新增数量统计图

（二）安全漏洞分布情况

从厂商分布来看，WordPress 基金会新增漏洞最多，有 127 个。各厂商漏洞数量分布如表 1 所示。

表 1 新增安全漏洞排名前五厂商统计表

序号	厂商名称	漏洞数量(个)	所占比例
1	WordPress 基金会	127	29.26%
2	荣耀	30	6.91%

3	腾达	12	2.76%
4	SESAMI	11	2.53%
5	诺基亚	7	1.61%

本周国内厂商漏洞 66 个，荣耀公司漏洞数量最多，有 30 个。国内厂商漏洞整体修复率为 75.76%。请受影响用户关注厂商修复情况，及时下载补丁修复漏洞。

从漏洞类型来看，SQL 注入类的安全漏洞占比最大，达到 16.13%。漏洞类型统计如表 2 所示。

表 2 漏洞类型统计表

序号	漏洞类型	漏洞数量（个）	所占比例
1	SQL 注入	70	16.13%
2	跨站脚本	44	10.14%
3	代码问题	28	6.45%
4	输入验证错误	11	2.53%
5	跨站请求伪造	10	2.30%
6	代码注入	10	2.30%
7	信息泄露	6	1.38%
8	路径遍历	2	0.46%
9	操作系统命令注入	2	0.46%
10	访问控制错误	1	0.23%
11	资源管理错误	1	0.23%
12	授权问题	1	0.23%
13	安全特征问题	1	0.23%
14	其他	247	56.91%

（三）安全漏洞危害等级与修复情况

本周共发布超危漏洞 22 个，高危漏洞 26 个，中危漏洞 382 个，低危漏洞 4 个。相应修复率分别为 72.73%、69.23%、70.42% 和 100.00%。根据补丁信息统计，合计 307 个漏洞已有修复补丁发布，整体修复率为 70.74%。详细情况如表 3 所示。

表 3 漏洞危害等级与修复情况

序号	危害等级	漏洞数量（个）	修复数量（个）	修复率
1	超危	22	16	72.73%
2	高危	26	18	69.23%
3	中危	382	269	70.42%
4	低危	4	4	100.00%
合计		434	307	70.74%

（四）本周重要漏洞实例

本周重要漏洞实例如表 4 所示。

表 4 本期重要漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例	是否修复	危害等级
1	代码注入	CNNVD-202312-2479	WordPress 基金会	WordPress plugin Verge3D Publishing and E-Commerce 代码注入漏洞	是	超危
2	代码问题	CNNVD-202312-2286	Apache 基金会	Apache OFBiz 代码问题漏洞	是	高危
3	跨站脚本	CNNVD-202312-2242	IBM	IBM Aspera Console 跨站脚本漏洞	是	高危

1. WordPress plugin Verge3D Publishing and E-Commerce 代码注入漏洞（CNNVD-202312-2479）

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 Verge3D Publishing and E-Commerce 4.5.2 版本及之前版本存在代码注入漏洞。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洞，参考链接：

<https://wordpress.org/plugins/verge3d/>

2. Apache OFBiz 代码问题漏洞（CNNVD-202312-2286）

Apache OFBiz 是美国阿帕奇（Apache）基金会的一套企业资源计划（ERP）系统。该系统提供了一整套基于 Java 的 Web 应用程序组件和工具。

Apache OFBiz 18.12.11 之前版本存在代码问题漏洞。攻击者利用该漏洞可以在未经授权的情况下操作相同的 uri 来执行服务器端请求伪造攻击。

目前厂商已发布升级补丁以修复漏洞，参考链接：

<https://lists.apache.org/thread/x5now4bk31lwf3k58kl96qvtjyxwp43q>

3. IBM Aspera Console 跨站脚本漏洞（CNNVD-202312-2242）

IBM Aspera Console 是美国国际商业机器（IBM）公司的一个基于 Web 的管理应用程序。

IBM Aspera Console 3.4.2 PL6 之前版本存在跨站脚本漏洞，该漏洞允许用户在 Web UI 中嵌入任意 JavaScript 代码，从而导致凭据泄露。

目前厂商已发布升级补丁以修复漏洞，参考链接：

<https://www.ibm.com/support/pages/node/7101252>

二、漏洞平台推送情况

本周 CNNVD 接收漏洞平台推送漏洞 80759 个。

表 5 本周漏洞平台推送情况

序号	漏洞平台	漏洞总量
1	漏洞盒子	49541
2	补天平台	30808
3	360 漏洞云	410
推送总计		80759

三、接报漏洞情况

本周 CNNVD 接报漏洞 1361 个，其中信息技术产品漏洞（通用型漏洞）864 个，网络信息系统漏洞（事件型漏洞）497 个。

表 6 本周漏洞报送情况

序号	报送单位	漏洞总量
1	内蒙古御网科技有限责任公司	491
2	北京山石网科信息技术有限公司	234
3	北京华云安信息技术有限公司	169
4	信元网络技术股份有限公司	123
5	内蒙古旌云科技有限公司	72
6	深信服科技股份有限公司	36
7	个人	27
8	北京启明星辰信息安全技术有限公司	19
9	湖南泛联新安信息科技有限公司	13

10	杭州美创科技股份有限公司	9
11	墨菲未来科技(北京)有限公司	9
12	南京聚铭网络科技有限公司	8
13	中电信数智科技有限公司	8
14	华为技术有限公司	7
15	北京墨云科技有限公司	6
16	博智安全科技股份有限公司	6
17	上海安识网络科技有限公司	6
18	西安四叶草信息技术有限公司	6
19	广州竞远安全技术股份有限公司	5
20	河南天祺信息安全技术有限公司	5
21	上海斗象信息科技有限公司	5
22	天翼数智科技（北京）有限公司	5
23	网宿科技股份有限公司	5
24	河南省鼎信信息安全等级测评有限公司	4
25	中兴通讯股份有限公司	4
26	北京奇虎科技有限公司	3
27	北京神州绿盟科技有限公司	3
28	北京有略安全技术有限公司	3
29	北京云起无垠科技有限公司	3
30	北京卓识网安技术股份有限公司	3
31	河南灵创电子科技有限公司	3
32	湖南中科安谷信息技术有限公司	3
33	华堡天建（天津）信息技术有限公司	3

34	浪潮电子信息产业股份有限公司	3
35	奇安信网神信息技术（北京）股份有限公司	3
36	清远职业技术学院	3
37	上海谋乐网络科技有限公司	3
38	深圳海云安网络安全技术有限公司	3
39	数字新时代（山东）数据科技服务有限公司	3
40	思而听（山东）网络科技有限公司	3
41	西安交大捷普网络科技有限公司	3
42	中国广电天津网络有限公司	3
43	北京国舜科技股份有限公司	2
44	北京镕瑞科技有限公司	2
45	北京天地和兴科技有限公司	2
46	北京长亭科技有限公司	2
47	赛尔网络有限公司	2
48	新华三技术有限公司	2
49	长扬科技（北京）股份有限公司	2
50	安徽长泰科技有限公司	1
51	北京安天网络安全技术有限公司	1
52	北京安信天行科技有限公司	1
53	北京中睿天下信息技术有限公司	1
54	成都卫士通信息安全技术有限公司	1
55	工业和信息化部电子第五研究所	1
56	杭州安恒信息技术股份有限公司	1
57	济南时代确信信息安全测评有限公司	1

58	江苏百达智慧网络科技有限公司	1
59	南京国云电力有限公司	1
60	上海安几科技有限公司	1
61	天地伟业技术有限公司	1
62	长春嘉诚信息技术股份有限公司	1
63	中国联合网络通信集团有限公司	1
报送总计		1361

四、收录漏洞通报情况

本周 CNNVD 收录漏洞通报 69 份。

表 7 本周漏洞通报情况

序号	报送单位	通报总量
1	中孚安全技术有限公司	16
2	内蒙古御网科技有限责任公司	6
3	奇安信网神信息技术（北京）股份有限公司	4
4	北京安普诺信息技术有限公司	3
5	中国广电天津网络有限公司	3
6	北京华云安信息技术有限公司	2
7	北京奇虎科技有限公司	2
8	北京知道创宇信息技术股份有限公司	2
9	河南灵创电子科技有限公司	2
10	湖北肆安科技有限公司	2
11	湖南泛联新安信息科技有限公司	2
12	江苏百达智慧网络科技有限公司	2
13	数字新时代（山东）数据科技服务有限公司	2

14	腾讯云计算（北京）有限责任公司	2
15	西安交大捷普网络科技有限公司	2
16	北方实验室（沈阳）股份有限公司	1
17	北京安博通科技股份有限公司	1
18	北京安天网络安全技术有限公司	1
19	北京山石网科信息技术有限公司	1
20	北京神州绿盟科技有限公司	1
21	北京时代新威信息技术有限公司	1
22	北京威努特技术有限公司	1
23	成都卫士通信息安全技术有限公司	1
24	烽台科技（北京）有限公司	1
25	杭州迪普科技股份有限公司	1
26	杭州美创科技股份有限公司	1
27	华堡天建（天津）信息技术有限公司	1
28	南京禾盾信息科技有限公司	1
29	上海矢安科技有限公司	1
30	深信服科技股份有限公司	1
31	深圳昂楷科技有限公司	1
32	新华三技术有限公司	1
收录总计		69