信息安全漏洞周报

（2026 年第 36 期 总第 849 期）

信息安全测评中心　　2026 年 9 月 6 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2026 年 8 月 31 日至 2026 年 9 月 6 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 2098 个。

接报漏洞情况

本周 CNNVD 接报漏洞 18874 个，其中信息技术产品漏洞（通用型漏洞）653 个，网络信息系统漏洞（事件型漏洞）13 个，漏洞平台推送漏洞 18208 个。

重大漏洞通报

WebPros cPanel 安全漏洞（CNNVD-2026-17225915、CVE-2026-65643）：成功利用漏洞的攻击者，可在目标服务器上以 root 身份执行任意代码，进而完全控制目标服务器。WebPros cPanel 11.110.0.141 之前版本受此漏洞影响。目前，WebPros 官方已发布新版本修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。

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 2098 个，漏洞新增数量有所下降。从厂商分布来看 Linux 基金会新增漏洞最多，有 188 个；从漏洞类型来看，授权问题类的安全漏洞占比最大，达到 16.49%。新增漏洞中，超危漏洞 226 个，高危漏洞 806 个，中危漏洞 908 个，低危漏洞 158 个。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 2098 个。

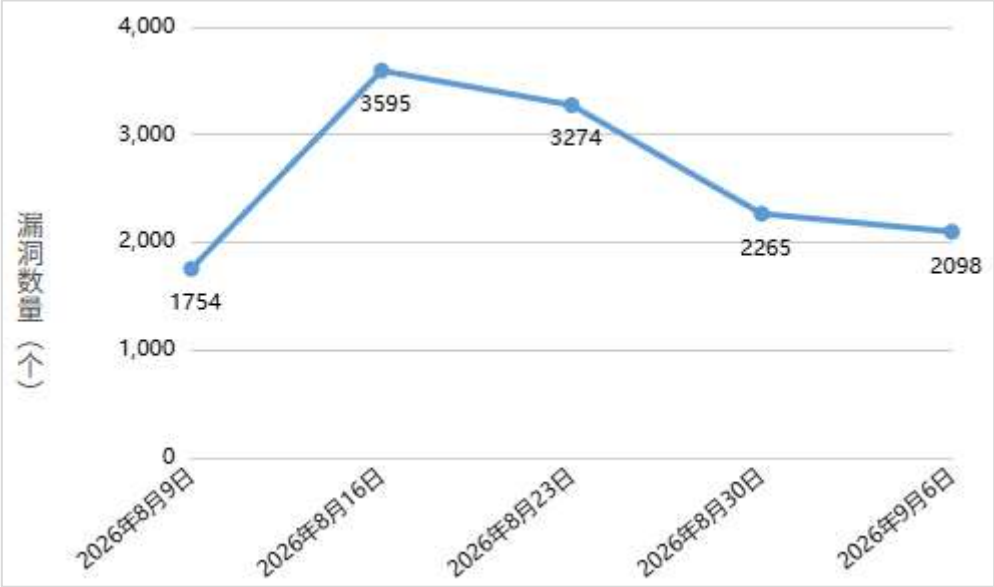

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Linux 基金会新增漏洞最多，有 188 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（项目）	漏洞数量（个）	所占比例
1	Linux 基金会	188	8.96%
2	WordPress 基金会	111	5.29%
3	吉翁电子	99	4.72%

4	Hewlett Packard Enterprise	86	4.10%
5	IBM	70	3.34%

本周国内厂商漏洞 167 个，吉翁电子公司漏洞数量最多，有 99 个。国内厂商漏洞整体修复率为 4.79%。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，授权问题类的安全漏洞占比最大，达到 16.49%。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	授权问题	346	16.49%
2	输入验证错误	199	9.49%
3	资源管理错误	162	7.72%
4	跨站脚本	162	7.72%
5	权限许可和访问控制问题	131	6.24%
6	缓冲区错误	106	5.05%
7	路径遍历	80	3.81%
8	命令注入	71	3.38%
9	信息泄露	50	2.38%
10	注入	49	2.34%
11	加密问题	48	2.29%
12	SQL 注入	39	1.86%
13	代码注入	28	1.33%
14	数字错误	28	1.33%
15	处理逻辑错误	27	1.29%

16	跨站请求伪造	23	1.10%
17	信任管理问题	22	1.05%
18	竞争条件问题	11	0.52%
19	日志信息泄露	7	0.33%
20	侧信道信息泄露	5	0.24%
21	后置链接	5	0.24%
22	格式化字符串错误	1	0.05%
23	其他	498	23.74%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 226 个，高危漏洞 806 个，中危漏洞 908 个，低危漏洞 158 个。相应修复率分别为 57.08%、78.78%、68.72%和 52.53%。根据补丁信息统计，合计 1471 个漏洞已有修复补丁发布，整体修复率为 70.11%。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	226	129	57.08%
2	高危	806	635	78.78%
3	中危	908	624	68.72%
4	低危	158	83	52.53%
合计		2098	1471	70.11%

（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	漏洞编号	危害等级
1	CNNVD-2026-69953794	超危

2	CNNVD-2026-47948241	高危
3	CNNVD-2026-36393757	高危

1. Google Chrome 资源管理错误漏洞（CNNVD-2026-69953794）

Google Chrome 是美国 Google 公司的一个跨平台 Web 浏览器。

Google Chrome 152.0.7977.75 之前版本存在资源管理错误漏洞，该漏洞源于内存释放后重用，攻击者利用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洞，参考链接：

https://www.google.com/chrome/

2. Microsoft Discovery Studio 输入验证错误漏洞（CNNVD-2026-47948241）

Microsoft Discovery Studio 是美国 Microsoft 公司的一款数据发现与分析平台。

Microsoft Discovery Studio 存在输入验证错误漏洞，该漏洞源于对用户提供的特殊元素中和不当，攻击者利用该漏洞可以泄露敏感信息。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62906

3. WordPress W3 Total Cache 跨站脚本漏洞（CNNVD-2026-36393757）

WordPress W3 Total Cache 是 WordPress 基金会的一款提升网站性能的缓存插件。

WordPress W3 Total Cache 2.10.5 版本及之前版本存在跨站脚本漏洞，该漏洞源于对用户的输入清理和输出转义不足，攻击者利用该漏洞可以在页面中注入任意 Web 脚本。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://wordpress.org/plugins/w3-total-cache/

（五） 本周重要人工智能漏洞实例

本周重要人工智能漏洞实例如表 5 所示。

表 5 本期重要人工智能漏洞实例

序号	漏洞编号	危害等级
1	CNNVD-2026-54571760	超危
2	CNNVD-2026-98622024	高危
3	CNNVD-2026-94820222	高危

1. Microsoft Azure AI Language Authoring 授权问题漏洞（CNNVD-2026-54571760）

Microsoft Azure AI Language Authoring 是美国 Microsoft 公司的一款人工智能语言处理与标注服务。

Microsoft Azure AI Language Authoring 存在授权问题漏洞，该漏洞源于关键功能缺少身份验证，攻击者利用该漏洞可以提升权限。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70352

2. vLLM 资源管理错误漏洞（CNNVD-2026-98622024）

vLLM 是一个开源的适用于 LLM 的高吞吐量和内存高效推理和服务引擎。

vLLM 0.17.0 及之前版本存在资源管理错误漏洞，该漏洞源于在获取用户提供的媒体 URL 时未限制响应数据的大小，攻击者利用该漏洞可以通过提供任意大文件的 URL 耗尽服务器内存，导致系统拒绝服务。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/vllm-project/vllm/releases

3. Ollama 服务端请求伪造漏洞（CNNVD-2026-94820222）

Ollama 是 Ollama 公司开源的一个可以在本地设备上运行、管理和自定义大语言模型的工具。

Ollama 0.30.0 版本至 0.33.2 版本存在服务端请求伪造漏洞，该漏洞源于在拉取 tensor-layer 模型时未能验证重定向目标，攻击者利用该漏洞可以获取敏感信息。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://ollama.com/

二、漏洞平台推送情况

本周 CNNVD 接收漏洞平台推送漏洞 18208 个。

表 6 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	10000
2	补天平台	7035
3	360 漏洞云	1173
推送总计		18208

三、接报漏洞情况

本周 CNNVD 接报漏洞 666 个，其中信息技术产品漏洞（通用型漏洞）653 个，网络信息系统漏洞（事件型漏洞）13 个。

表 7 本周漏洞报送情况

序号	报送单位	漏洞总量
1	个人	133
2	北京长亭科技有限公司	75
3	北京微步在线科技有限公司	33
4	广州纬安科技有限公司	24
5	四川溯蓉信创科技有限公司	24
6	三六零数字安全科技集团有限公司	24
7	奇安信网神信息技术（北京）股份有限公司	22
8	北京启明星辰信息安全技术有限公司	21
9	南京轻舟共联信息科技有限公司	17
10	上海碳泽信息科技有限公司	17
11	大川信安（成都）科技有限公司	16
12	深信服科技股份有限公司	16
13	新华三技术有限公司	15
14	中兴通讯股份有限公司	14
15	西安捷润数码科技有限公司	11
16	北京安天网络安全技术有限公司	9
17	北京世纪超星信息技术发展有限责任有限公司	9
18	浙江极安信息科技有限公司	7
19	成都安美勤信息技术股份有限公司	7
20	腾讯云计算（北京）有限责任有限公司	7
21	复旦大学系统软件与安全实验室	6
22	江苏嘉玖信息科技有限公司	6

23	中资网络信息安全科技有限公司	6
24	超聚变数字技术股份有限公司	5
25	广东省信息安全测评中心	5
26	浙江大华技术股份有限公司	5
27	深圳市魔方安全科技有限公司	5
28	成都创信华通信息技术有限公司	4
29	北京浩瀚深度信息技术股份有限公司	4
30	北京天融信网络安全技术有限公司	4
31	广州竞远安全技术股份有限公司	4
32	上海戟安科技有限公司	4
33	西藏熙安信息技术有限公司	4
34	北京猎鹰安全科技有限公司	4
35	河南天祺信息安全技术有限公司	4
36	统信软件技术有限公司	3
37	厦门快快网络科技有限公司	3
38	上海矢安科技股份有限公司	3
39	河南东方云盾信息技术有限公司	3
40	江苏翔信信息安全技术有限公司	3
41	上海壹安至行技术有限公司	3
42	中乾建技术有限公司	3
43	中移系统集成有限公司	3
44	江苏力可信网络科技有限公司	3
45	湖南泛联新安信息科技有限公司	3
46	浙江豪联信息科技有限公司	3

47	内蒙古旌云科技有限公司	2
48	信元网络技术股份有限公司	2
49	博智安全科技股份有限公司	2
50	北京凝思软件股份有限公司	2
51	北京五一嘉峪科技有限公司	2
52	杭州安恒信息技术股份有限公司	2
53	青海数境科技有限公司	2
54	中电智安科技有限公司	2
55	中建数字科技有限公司	2
56	中國通信服務香港有限公司	2
57	零熵科技（甘肃）有限公司	2
58	国家电投集团数字科技有限公司	2
59	中国电信股份有限公司研究院	2
60	北京时代新威信息技术有限公司	2
61	北京磐石安科技有限公司	2
62	内蒙古思沃科技有限公司	2
63	北京神州绿盟科技有限公司	2
64	北京安普诺信息技术有限公司	2
65	陕西思安信息网络安全有限公司	2
66	天津市滨智启源信息技术有限公司	1
67	广州锦行网络科技有限公司	1
68	杭州迪普科技股份有限公司	1
69	杭州海康威视数字技术股份有限公司	1
70	宝鸡市阳光网络技术有限公司	1

71	湖南浩基信息技术有限公司	1
72	深圳九有数据库有限公司	1
73	中国大唐集团科学技术研究总院有限公司	1
74	内蒙古启航未来科技有限公司	1
75	海南省通信产业服务有限公司	1
76	深圳市能信安科技股份有限公司	1
77	安恒愿景（成都）信息科技有限公司	1
78	北京天融信教育科技有限公司	1
79	龙源电力集团股份有限公司	1
80	江苏君立华域信息安全技术股份有限公司	1
81	墨菲未来科技（北京）有限公司	1
82	泉州延陵信息技术有限公司	1
83	广州松杨云创科技有限公司	1
84	国核自仪网络安全技术（上海）有限责任公司	1
85	天津市兴先道科技有限公司	1
86	甘肃青鸾信息技术有限公司	1
87	山西晋信安科技有限公司	1
88	南京南瑞网络安全技术有限公司	1
89	北京前瞻人工智能安全与治理研究院	1
报送总计		666

四、收录漏洞通报情况

本周 CNNVD 收录漏洞通报 190 份。

表 8 本周漏洞通报情况

序号	报送单位	通报总量

1	中国银联股份有限公司	40
2	泉州延陵信息技术有限公司	30
3	奇安信网神信息技术（北京）股份有限公司	26
4	南京赛宁信息技术有限公司	12
5	江苏嘉玖信息科技有限公司	8
6	中移系统集成有限公司	6
7	深圳九有数据库有限公司	6
8	沈阳帆网信息技术有限公司	5
9	西安捷润数码科技有限公司	4
10	杭州迪普科技股份有限公司	4
11	内蒙古浩辉信息科技有限公司	3
12	内蒙古虹安信息科技有限公司	3
13	北京金源动力信息化测评技术有限公司	3
14	天谋科技（北京）有限公司	3
15	华易数安科技(吉林省)有限公司	3
16	上海直画科技有限公司	3
17	北京五一嘉峪科技有限公司	3
18	北京上元信安技术有限公司	3
19	零熵科技（甘肃）有限公司	2
20	博智安全科技股份有限公司	2
21	西藏熙安信息技术有限公司	2
22	北京安信天行科技有限公司	1
23	三六零数字安全科技集团有限公司	1
24	湖南麒麟信安科技股份有限公司	1

25	联通（江西）产业互联网有限公司	1
26	沈阳汉林科技有限公司	1
27	广州非凡信息安全技术有限公司	1
28	超聚变数字技术股份有限公司	1
29	江苏君立华域信息安全技术股份有限公司	1
30	阿里云计算有限公司	1
31	内蒙古旌云科技有限公司	1
32	厦门快快网络科技有限公司	1
33	北京天融信网络安全技术有限公司	1
34	北京长亭科技有限公司	1
35	陕西青山四纪信息技术有限公司	1
36	成都卫士通信息安全技术有限公司	1
37	中国联合网络通信有限公司深圳市分公司	1
38	北京云科安信科技有限公司	1
39	华为技术有限公司	1
40	中乾建技术有限公司	1
收录总计		190

五、重大漏洞通报

CNNVD 关于 WebPros cPanel 安全漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 WebPros cPanel 安全漏洞（CNNVD-2026-17225915、CVE-2026-65643）情况的报送。成功利用漏洞的攻击者，可在目标服务器上以 root 身份执行任意代码，进而完全控制目标服务器。WebPros cPanel 11.110.0.141 之前版本受此漏洞影响。目前，WebPros 官方已发布

新版本修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。

1.漏洞介绍

WebPros cPanel 是 WebPros 公司的一款面向服务器和网站管理的 Web 主机控制面板软件。漏洞源于 WebPros cPanel 服务器后端在处理域名相关参数的流程中存在动态代码注入缺陷，持有普通 cPanel 账户的攻击者在登录以后，可调用相应 API 触发该漏洞，进而在服务器上以 root 身份执行任意代码。

2.危害影响

WebPros cPanel 11.110.0.141 之前版本受此漏洞影响。

3.修复建议

目前，WebPros 官方已发布新版本修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。官方参考链接如下：

https://support.cpanel.net/hc/en-us/articles/42959571221527-Security-CVE-2026-65643-Park-API-Vulnerability-August-27-2026