信息安全漏洞周报

（2026 年第 40 期 总第 853 期）

信息安全测评中心　　2026 年 10 月 11 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2026 年 10 月 5 日至 2026 年 10 月 11 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 2550 个。

接报漏洞情况

本周 CNNVD 接报漏洞 34521 个，其中信息技术产品漏洞（通用型漏洞）435 个，网络信息系统漏洞（事件型漏洞）6 个，漏洞平台推送漏洞 34080 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 2550 个，漏洞新增数量有所上升。从厂商分布来看谷歌公司新增漏洞最多，有 298 个；从漏洞类型来看，授权问题类的安全漏洞占比最大，达到 19.22%。新增漏洞中，超危漏洞 313 个，高危漏洞 897 个，中危漏洞 1211 个，低危漏洞 129 个。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 2550 个。

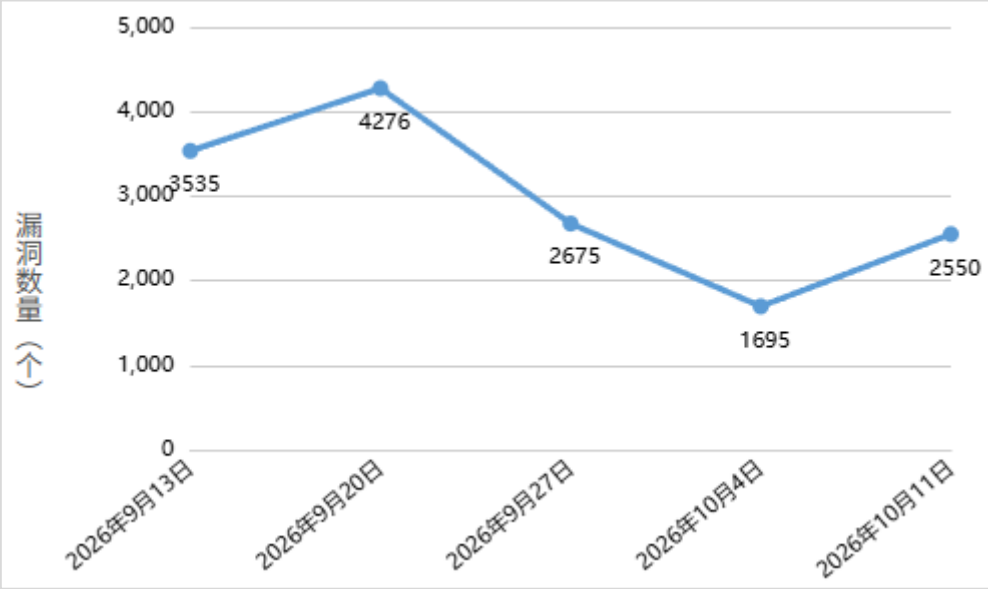


图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，谷歌公司新增漏洞最多，有 298 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	谷歌	298	11.69%
2	Linux 基金会	220	8.63%
3	WordPress 基金会	176	6.90%

4	IBM	108	4.24%
5	jeecgboot	60	2.35%

本周国内厂商漏洞 54 个，联发科技公司漏洞数量最多，有 31 个。国内厂商漏洞整体修复率为 83.33%。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 19.22%。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	490	19.22%
2	资源管理错误	240	9.41%
3	跨站脚本	208	8.16%
4	缓冲区错误	206	8.08%
5	输入验证错误	185	7.25%
6	权限许可和访问控制问题	105	4.12%
7	路径遍历	90	3.53%
8	信息泄露	81	3.18%
9	注入	72	2.82%
10	代码注入	62	2.43%
11	SQL 注入	61	2.39%
12	加密问题	57	2.24%
13	命令注入	53	2.08%
14	处理逻辑错误	52	2.04%
15	竞争条件问题	35	1.37%

16	数字错误	30	1.18%
17	信任管理问题	29	1.14%
18	跨站请求伪造	14	0.55%
19	日志信息泄露	9	0.35%
20	侧信道信息泄露	9	0.35%
21	后置链接	9	0.35%
22	调试信息泄露	4	0.16%
23	格式化字符串错误	1	0.04%
24	其他	448	17.57%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 313 个，高危漏洞 897 个，中危漏洞 1211 个，低危漏洞 129 个。相应修复率分别为 64.22%、75.70%、80.84% 和 61.24%。根据补丁信息统计，合计 1938 个漏洞已有修复补丁发布，整体修复率为 76.00%。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	313	201	64.22%
2	高危	897	679	75.70%
3	中危	1211	979	80.84%
4	低危	129	79	61.24%
合计		2550	1938	76.00%

（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-2026-55951847	超危
2	CNNVD-2026-96580885	高危
3	CNNVD-2026-37041471	高危

1. Google Chrome 资源管理错误漏洞（CNNVD-2026-55951847）

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

Google Chrome 155.0.8059.39 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通过特制 HTML 页面在沙箱外执行任意代码。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_086471744.html

2. Dell Secure Connect Gateway Policy Manager 授权问题漏洞（CNNVD-2026-96580885）

Dell Secure Connect Gateway Policy Manager 是美国 Dell 公司的一款企业级安全连接网关策略管理软件。

Dell Secure Connect Gateway Policy Manager 5.34.00.16 之前版本存在授权问题漏洞，该漏洞源于没有限制身份验证尝试的次数，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://www.dell.com/support/kbdoc/en-ca/000503592/dsa-2026-385-security-update-for-dell-secure-connect-gateway-policy-manager-multiple-vulnerabilities?msockid=3021cac2195069ed3194ddad186a68f9

3. IBM Guardium Data Protection SQL 注入漏洞（CNNVD-2026-37041471）

IBM Guardium Data Protection 是美国 IBM 公司的一款防止敏感数据泄露与丢失的数据安全防护软件。

IBM Guardium Data Protection 12.2.2 版本和 12.1 版本存在 SQL 注入漏洞，该漏洞源于对 SQL 命令中的特殊元素中和不当，攻击者利用该漏洞可以执行任意 SQL 命令。

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/7288832

（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-2026-73253135	超危
2	CNNVD-2026-28065481	高危
3	CNNVD-2026-62101954	高危

1. IBM Langflow OSS 代码注入漏洞（CNNVD-2026-73253135）

IBM Langflow OSS 是美国 IBM 公司的一个可视化搭建语言模型应用工作流的平台。

IBM Langflow OSS 1.0.0 版本至 1.12.2 版本存在代码注入漏洞，该漏洞源于对操作系统命令中使用的特殊元素中和不当，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.ibm.com/support/pages/node/7290694

2. LMCache 授权问题漏洞（CNNVD-2026-28065481）

LMCache 是一款面向大语言模型推理的缓存加速系统。

LMCache 0.5.5 及之前版本存在授权问题漏洞，该漏洞源于多进程协调器缺少身份验证，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://lmcache.ai/

3. Obot AI Obot 信任管理问题漏洞（CNNVD-2026-62101954）

Obot AI Obot 是一款开源的人工智能聊天机器人软件。

Obot AI Obot 0.12.0 版本至 0.26.2 之前版本存在信任管理问题漏洞，该漏洞源于对凭证保护不足，攻击者利用该漏洞可以获取明文 API 密钥或令牌并滥用于后端服务。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/obot-platform/obot/security/advisories/GHSA-q5wf-87f5-cxgq

二、漏洞平台推送情况

本周 CNNVD 接收漏洞平台推送漏洞 34080 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	30210
2	补天平台	2857
3	360 漏洞云	1013
推送总计		34080

三、接报漏洞情况

本周 CNNVD 接报漏洞 441 个，其中信息技术产品漏洞（通用型漏洞）435 个，网络信息系统漏洞（事件型漏洞）6 个。

表 7 本周漏洞报送情况

序号	报送单位	漏洞总量

1	个人	88
2	零日信安（武汉市）技术有限责任有限公司	52
3	广州纬安科技有限公司	30
4	北京长亭科技有限公司	23
5	杭州海康威视数字技术股份有限公司	19
6	深圳市计量质量检测研究院	14
7	华清未央（北京）科技有限公司	13
8	内蒙古洞明科技有限公司	11
9	内蒙古旌云科技有限公司	11
10	浙江大华技术股份有限公司	9
11	北京国御科技有限公司	8
12	湖南浩基信息技术有限公司	8
13	中乾建技术有限公司	7
14	三六零数字安全科技集团有限公司	7
15	北方实验室（沈阳）股份有限公司	6
16	北京天融信网络安全技术有限公司	6
17	北京神州绿盟科技有限公司	6
18	中兴通讯股份有限公司	6
19	杭州安恒信息技术股份有限公司	5
20	上海安几科技有限公司	5
21	北京微步在线科技有限公司	5
22	河南天祺信息安全技术有限公司	5
23	南方电网数字电网集团（贵州）有限公司	5
24	江苏力可信网络科技有限公司	5

25	联通数字科技有限公司	4
26	南京国云电力有限公司	4
27	安恒愿景（成都）信息科技有限公司	4
28	北京天地和兴科技股份有限公司	4
29	安徽溯源电子科技有限公司	3
30	浙江豪联信息科技有限公司	3
31	山东省网安数字科技有限公司	3
32	远江盛邦安全科技集团股份有限公司	3
33	内蒙古宇世信息技术有限公司	3
34	恒安嘉新（北京）科技股份	3
35	内蒙古万邦信息安全技术有限公司	3
36	浙江东安检测技术有限公司	3
37	西安四叶草信息技术有限公司	3
38	博智安全科技股份有限公司	3
39	奇安信网神信息技术（北京）股份有限公司	3
40	北京安华金和科技有限公司	2
41	长沙博卓信息技术有限公司	2
42	成都创信华通信息技术有限公司	2
43	山东广迪信息科技有限公司	2
44	联通（江西）产业互联网有限公司	2
45	中国第一汽车集团有限公司	2
46	新华三技术有限公司	2
47	北京威努特技术有限公司	2
48	深圳九有数据库有限公司	2

49	建信金融科技有限责任有限公司	1
50	济南三泽信息安全测评有限公司	1
51	深圳市博通智能技术有限公司	1
52	思而听（山东）网络科技有限公司	1
53	合肥掌安网络科技有限公司	1
54	北京锐服信科技有限公司	1
55	中电智安科技有限公司	1
56	厦门快快网络科技有限公司	1
57	零熵科技（甘肃）有限公司	1
58	华为技术有限公司	1
59	联通（广东）网络信息安全科技有限公司	1
60	广东省信息安全测评中心	1
61	河南东方云盾信息技术有限公司	1
62	内蒙古亚信安联科技有限公司	1
63	内蒙古数字安全科技有限公司	1
64	广州松杨云创科技有限公司	1
65	福建南玲科技有限公司	1
66	北京启明星辰信息安全技术有限公司	1
67	河南省鼎信信息安全等级测评有限公司	1
68	云南蓝队云计算有限公司	1
报送总计		441

四、收录漏洞通报情况

本周 CNNVD 收录漏洞通报 146 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	19
2	奇安信网神信息技术（北京）股份有限公司	19
3	泉州延陵信息技术有限公司	15
4	南京赛宁信息技术有限公司	13
5	杭州迪普科技股份有限公司	9
6	江苏嘉玖信息科技有限公司	8
7	陕西慧缘网络科技有限公司	6
8	重庆巽诺科技有限公司	5
9	内蒙古宇世信息技术有限公司	5
10	华清未央（北京）科技有限公司	5
11	泉州吉胜信息技术有限公司	4
12	南方电网数字电网集团（贵州）有限公司	4
13	河南天祺信息安全技术有限公司	3
14	阿里云计算有限公司	2
15	河南东方云盾信息技术有限公司	2
16	北京奇虎科技有限公司	2
17	上海见形信息科技有限公司	2
18	合肥掌安网络科技有限公司	2
19	深圳市博通智能技术有限公司	2
20	北京安天网络安全技术有限公司	2
21	深圳市网安计算机安全检测技术有限公司	2
22	天津市兴先道科技有限公司	2
23	深圳市计量质量检测研究院	1

24	北京容辉智信科技有限公司	1
25	河南省鼎信信息安全等级测评有限公司	1
26	江苏君立华域信息安全技术股份有限公司	1
27	西安交大捷普网络科技有限公司	1
28	青鸾信息技术（青海）有限公司	1
29	沈阳汉林科技有限公司	1
30	恒安嘉新（北京）科技股份	1
31	天谋科技（北京）有限公司	1
32	重庆智网科技产业发展有限公司信息通信分公司	1
33	北京长亭科技有限公司	1
34	甘肃安信信息安全技术有限公司	1
35	锐捷网络股份有限公司	1
收录总计		146