信息安全漏洞周报

（2026 年第 42 期 总第 855 期）

信息安全测评中心　　2026 年 10 月 25 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2026 年 10 月 19 日至 2026 年 10 月 25 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 3806 个。

接报漏洞情况

本周 CNNVD 接报漏洞 35964 个，其中信息技术产品漏洞（通用型漏洞）600 个，网络信息系统漏洞（事件型漏洞）4 个，漏洞平台推送漏洞 35360 个。

重大漏洞通报

PHP 资源管理错误漏洞（CNNVD-2026-75300632、CVE-2026-109618）、（CNNVD-2026-41545346、CVE-2026-109619）：成功利用漏洞的攻击者，可通过构造恶意 HTTP 请求实现内存泄露，进而远程执行代码。PHP 多个版本均受此漏洞影响。目前，PHP 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 3806 个，漏洞新增数量有所下降。从厂商分布来看 Oracle 公司新增漏洞最多，有 1078 个；从漏洞类型来看，授权问题类的安全漏洞占比最大，达到 11.09%。新增漏洞中，超危漏洞 491 个，高危漏洞 1357 个，中危漏洞 1629 个，低危漏洞 329 个。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 3806 个。

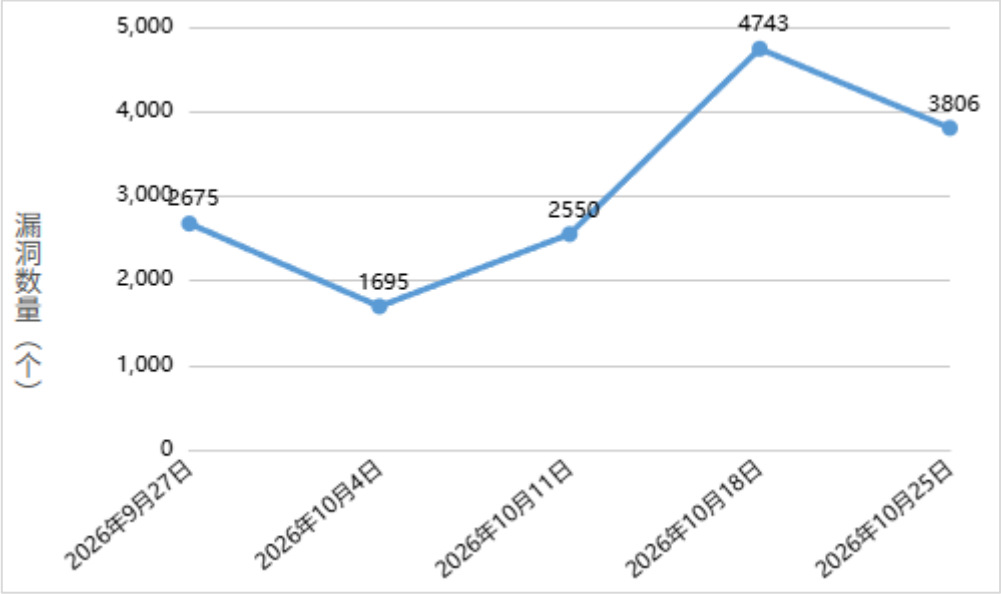


图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Oracle 公司新增漏洞最多，有 1078 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	Oracle	1078	28.32%
2	谷歌	361	9.49%
3	Linux 基金会	220	5.78%

4	Apache 基金会	153	4.02%
5	WordPress 基金会	79	2.08%

本周国内厂商漏洞 127 个，吉翁电子公司漏洞数量最多，有 33 个。国内厂商漏洞整体修复率为 47.24%。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 11.09%。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	422	11.09%
2	缓冲区错误	366	9.62%
3	资源管理错误	358	9.41%
4	输入验证错误	276	7.25%
5	权限许可和访问控制问题	177	4.65%
6	跨站脚本	164	4.31%
7	路径遍历	113	2.97%
8	信息泄露	101	2.65%
9	加密问题	75	1.97%
10	命令注入	53	1.39%
11	注入	42	1.10%
12	代码注入	41	1.08%
13	SQL 注入	40	1.05%
14	处理逻辑错误	38	1.00%
15	数字错误	31	0.81%

16	信任管理问题	29	0.76%
17	跨站请求伪造	26	0.68%
18	竞争条件问题	23	0.60%
19	后置链接	19	0.50%
20	日志信息泄露	12	0.32%
21	侧信道信息泄露	7	0.18%
22	调试信息泄露	1	0.03%
23	其他	1392	36.57%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 491 个，高危漏洞 1357 个，中危漏洞 1629 个，低危漏洞 329 个。相应修复率分别为 82.69%、90.57%、89.93%和 77.81%。根据补丁信息统计，合计 3356 个漏洞已有修复补丁发布，整体修复率为 88.18%。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	491	406	82.69%
2	高危	1357	1229	90.57%
3	中危	1629	1465	89.93%
4	低危	329	256	77.81%
合计		3806	3356	88.18%

（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-2026-97813474	超危

2	CNNVD-2026-75220766	高危
3	CNNVD-2026-29975530	高危

1. Google Chrome 资源管理错误漏洞（CNNVD-2026-97813474）

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

Google Chrome 156.0.8078.47 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问题，攻击者利用该漏洞可以通过特制的 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_02018666648.html

2. Apache CouchDB 资源管理错误漏洞（CNNVD-2026-75220766）

Apache CouchDB 是美国 Apache 基金会的一款服务端软件产品。

Apache CouchDB 3.5.2 及之前版本存在资源管理错误漏洞，该漏洞源于在 gzip 解压缩过程中没有限制解压缩大小，攻击者利用该漏洞可以通过耗尽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://lists.apache.org/thread.html/pj83174r8f8f64odf47fwhozbfjtot0f

3. Dell Application Store 授权问题漏洞（CNNVD-2026-29975530）

Dell Application Store 是美国 Dell 公司的一款应用程序分发与下载管理软件。

Dell Application Store 26.05.0.7 之前版本存在授权问题漏洞，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.dell.com/support/kbdoc/en-us/000506927/dsa-2026-411-security-update-for-dell-application-store-for-multiple-vulnerabilities

（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-2026-61426883	超危
2	CNNVD-2026-55699613	高危
3	CNNVD-2026-54157834	高危

1. Amazon sagemaker-python-sdk 授权问题漏洞（CNNVD-2026-61426883）

Amazon sagemaker-python-sdk 是美国 Amazon 公司开源的一个用于在 Amazon SageMaker 上训练和部署机器学习模型的库。

Amazon sagemaker-python-sdk V3 3.10.0 之前版本和 V2 2.257.3 之前版本存在授权问题漏洞，该漏洞源于 default_bucket 函数缺少通信信道的来源验证，攻击者利用该漏洞可以执行代码并获取 IAM 凭据。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/aws/sagemaker-python-sdk/security/advisories/GHSA-5rx8-8fr2-f855

2. sgl-project SGLang 资源管理错误漏洞（CNNVD-2026-55699613）

sgl-project SGLang 是 sgl-project 组织开源的一个用于加速大模型推理的编程语言与运行时系统。

sgl-project SGLang 0.5.22 及之前版本存在资源管理错误漏洞，该漏洞源于内存分配不当，攻击者利用该漏洞可以耗尽内存导致系统终止运行。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/sgl-project/sglang/releases

3. vLLM 资源管理错误漏洞（CNNVD-2026-54157834）

vLLM 是 vLLM 组织开源的一个适用于 LLM 的高吞吐量和内存高效推理和服务引擎。

vLLM 0.7.3 版本至 0.31.0 之前版本存在资源管理错误漏洞，该漏洞源于在 Isaac、InternVL、H2OVL 等处理器中允许设置较大的图像尺寸、补丁数量、裁剪数量或帧数值，攻击者利用该漏洞可以导致内存耗尽并终止共享服务器。

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/security/advisories/GHSA-gx7p-2j49-hfq4

二、漏洞平台推送情况

本周 CNNVD 接收漏洞平台推送漏洞 35360 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	26732
2	补天平台	7561
3	360 漏洞云	1067
推送总计		35360

三、接报漏洞情况

本周 CNNVD 接报漏洞 604 个，其中信息技术产品漏洞（通用型漏洞）600 个，网络信息系统漏洞（事件型漏洞）4 个。

表 7 本周漏洞报送情况

序号	报送单位	漏洞总量
1	零日信安（武汉市）技术有限责任有限公司	89
2	个人	82
3	广州纬安科技有限公司	59
4	三六零数字安全科技集团有限公司	27
5	深圳市计量质量检测研究院	16
6	杭州安恒信息技术股份有限公司	15
7	武汉金银湖实验室	13
8	浙江极安信息科技有限公司	13
9	北京天融信网络安全技术有限公司	13
10	天翼安全科技有限公司	12
11	北京威努特技术有限公司	12
12	北京启明星辰信息安全技术有限公司	11
13	成都安美勤信息技术股份有限公司	11
14	中资网络信息安全科技有限公司	10
15	大川信安（成都）科技有限公司	10
16	内蒙古洞明科技有限公司	9
17	合肥掌安网络科技有限公司	9
18	亚信科技（成都）有限公司	8
19	苏州棱镜七彩信息科技有限公司	7

20	成都创信华通信息技术有限公司	7
21	建信金融科技有限责任有限公司	7
22	中科数测固源科技（安徽）有限公司	6
23	北京神州绿盟科技有限公司	6
24	天津恒御科技有限公司	6
25	泉州吉胜信息技术有限公司	5
26	钛信（上海）信息科技有限公司	5
27	北京天地和兴科技股份有限公司	5
28	北京小佑网络科技有限公司	5
29	北京长亭科技有限公司	5
30	陕西思安信息网络安全有限公司	5
31	江苏嘉玖信息科技有限公司	5
32	内蒙古大坤信息技术有限公司	4
33	浙江东安检测技术有限公司	4
34	国网湖北省电力有限公司电力科学研究院	4
35	山东数悦信息技术有限公司	4
36	北京凝思软件股份有限公司	4
37	上海斗象信息科技有限公司	4
38	北京墨云科技有限公司	4
39	北京国御科技有限公司	4
40	广东为辰信息科技有限公司	3
41	锐捷网络股份有限公司	3
42	成都卫士通信息安全技术有限公司	3
43	河南东方云盾信息技术有限公司	3

44	南方电网数字电网集团（贵州）有限公司	3
45	湖南匡安网络技术有限公司	3
46	重庆巽诺科技有限公司	3
47	湖南麒麟信安科技股份有限公司	3
48	扬州大自然网络信息有限公司	3
49	北京华云安信息技术有限公司	2
50	云南南天电子信息产业股份有限公司	2
51	济南三泽信息安全测评有限公司	2
52	天讯瑞达通信技术有限公司	2
53	漳州市新天一网络科技有限公司	2
54	北方实验室（沈阳）股份有限公司	2
55	安恒愿景（成都）信息科技有限公司	2
56	中兴通讯股份有限公司	2
57	贵州芃星科技有限公司	2
58	广东省信息安全测评中心	2
59	江苏网擎信息技术有限公司	2
60	成都数默科技有限公司	2
61	华易数安科技(吉林省)有限公司	2
62	深信服科技股份有限公司	2
63	北京安华金和科技有限公司	1
64	山西晋信安科技有限公司	1
65	金盾检测技术股份有限公司	1
66	北京飞轮数据科技有限公司	1
67	内蒙古电力（集团）有限责任公司内蒙古电力科学研究院分公司	1

68	零熵科技（甘肃）有限公司	1
69	北京珞安科技有限责任公司	1
70	江苏正信信息安全测试有限公司	1
71	维安（山东）数字技术有限公司	1
72	超聚变数字技术股份有限公司	1
73	国汀信息科技（北京）有限公司	1
74	北京赛博昆仑科技有限公司	1
75	北京微步在线科技有限公司	1
76	内蒙古奥创科技有限公司	1
77	任子行网络技术股份有限公司	1
78	华为技术有限公司	1
79	浙江大华技术股份有限公司	1
80	联通（广东）网络信息安全科技有限公司	1
81	中国联合网络通信有限公司深圳市分公司	1
82	联通（安徽）产业互联网有限公司	1
83	湖南安服信息技术有限公司	1
84	上海戎磐网络科技有限公司	1
85	浙江国利网安科技有限公司	1
86	厦门快快网络科技有限公司	1
报送总计		604

四、收录漏洞通报情况

本周 CNNVD 收录漏洞通报 220 份。

表 8 本周漏洞通报情况

序号	报送单位	通报总量

1	奇安信网神信息技术（北京）股份有限公司	28
2	江苏嘉玖信息科技有限公司	11
3	北京国御科技有限公司	9
4	中国银联股份有限公司	8
5	甘肃安信信息安全技术有限公司	8
6	浙江国利网安科技有限公司	8
7	深圳市网安计算机安全检测技术有限公司	8
8	泉州延陵信息技术有限公司	7
9	四川溯蓉信创科技有限公司	6
10	成都数默科技有限公司	6
11	钛信（上海）信息科技有限公司	6
12	浙江极安信息科技有限公司	6
13	湖南匡安网络技术有限公司	5
14	北京信联数安科技有限公司	5
15	北京奇虎科技有限公司	4
16	深信服科技股份有限公司	4
17	维安（山东）数字技术有限公司	3
18	江苏正信信息安全测试有限公司	3
19	博智安全科技股份有限公司	3
20	内蒙古大坤信息技术有限公司	3
21	零熵科技（甘肃）有限公司	3
22	江西神舟信息安全评估中心有限公司	3
23	青鸾信息技术（青海）有限公司	3
24	南京禾盾信息科技有限公司	3

25	杭州安恒信息技术股份有限公司	2
26	广州纬安科技有限公司	2
27	苏州棱镜七彩信息科技有限公司	2
28	北京启明星辰信息安全技术有限公司	2
29	上海碳泽信息科技有限公司	2
30	北京安天网络安全技术有限公司	2
31	国网湖北省电力有限公司电力科学研究院	2
32	北京山石网科信息技术有限公司	2
33	天谋科技（北京）有限公司	2
34	西安交大捷普网络科技有限公司	2
35	北京自然原数科技有限公司	2
36	擎境（日照）网络信息科技有限责任公司	2
37	山东广迪信息科技有限公司	2
38	敦和安全科技（武汉）有限公司	2
39	北京长亭科技有限公司	2
40	湖北东方网盾信息安全技术有限公司	2
41	统信软件技术有限公司	2
42	漳州市新天一网络科技有限公司	2
43	河南省鼎信信息安全等级测评有限公司	2
44	北京神州绿盟科技有限公司	2
45	云南蓝队云计算有限公司	2
46	陕西青山四纪信息技术有限公司	1
47	成都安美勤信息技术股份有限公司	1
48	北京安华金和科技有限公司	1

49	上海矢安科技有限公司	1
50	杭州迪普科技股份有限公司	1
51	西安隆基智能技术有限公司	1
52	成都卫士通信息安全技术有限公司	1
53	远江盛邦安全科技集团股份有限公司	1
54	新华三技术有限公司	1
55	中国联合网络通信有限公司深圳市分公司	1
56	浙江大华技术股份有限公司	1
57	华为技术有限公司	1
58	厦门快快网络科技有限公司	1
59	超聚变数字技术股份有限公司	1
60	北京天融信网络安全技术有限公司	1
61	建信金融科技有限责任有限公司	1
62	北京飞轮数据科技有限公司	1
63	北京威努特技术有限公司	1
64	上海戎磐网络科技有限公司	1
65	北京容辉智信科技有限公司	1
66	浪潮电子信息产业股份有限公司	1
67	内蒙古电力（集团）有限责任公司内蒙古电力科学研究院分公司	1
68	北京金源动力信息化测评技术有限公司	1
69	西安安迈信科科技有限公司	1
70	南方电网数字电网集团（贵州）有限公司	1
收录总计		220

五、重大漏洞通报

CNNVD 关于 PHP 操作系统命令注入漏洞的通报

近日，国家信息安全漏洞库（CNNVD）收到关于 PHP 资源管理错误漏洞（CNNVD-2026-75300632、CVE-2026-109618）（CNNVD-2026-41545346、CVE-2026-109619）情况的报送。成功利用漏洞的攻击者，可通过构造恶意 HTTP 请求实现内存泄露，进而远程执行代码。PHP 多个版本均受此漏洞影响。目前，PHP 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

PHP 是 PHP 团队开源的一种在服务器端执行的脚本语言。PHP 存在资源管理错误漏洞，其中（CNNVD-2026-75300632、CVE-2026-109618）源于使用 longjmp()处理内存时错误，导致请求内存在分配前处于未初始化状态。（CNNVD-2026-41545346、CVE-2026-109619）源于 PHP 在全局状态请求结束后未正确重置，使后续请求在正常初始化之前访问已释放的请求内存。未经认证的攻击者可利用漏洞，通过构造恶意 HTTP 请求实现内存泄露，进而远程执行代码。

2.危害影响

PHP 8.2.35 版本之前的 8.2.x 版本、8.3.36 版本之前的 8.3.x 版本、8.4.27 版本之前的 8.4.x 版本和 8.5.12 版本之前的 8.5.x 版本均受此漏洞影响。

3.修复建议

目前，PHP 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：

https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp