信息安全漏洞周报

（2020 年第 49 期 总第 553 期）

信息安全测评中心　　2020 年 12 月 20 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 12 月 14 日至 2020 年 12 月 20 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 369 个，与上周（510 个）相比减少了 27.65%。

接报漏洞情况

本周 CNNVD 接报漏洞 12509 个，其中信息技术产品漏洞（通用型漏洞）27 个，网络信息系统漏洞（事件型漏洞）12482 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 369 个，漏洞新增数量有所下降。从厂商分布来看 Apple 公司新增漏洞最多，有 44 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 10.03%。新增漏洞中，超危漏洞 67 个，高危漏洞 111 个，中危漏洞 178 个，低危漏洞 13 个。相应修复率分别为 41.79%、92.79%、88.20%和 100.00%。根据补丁信息统计，合计 301 个漏洞已有修复补丁发布，整体修复率为 81.57%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 369 与上周（510 个）相比减少了 27.65%。

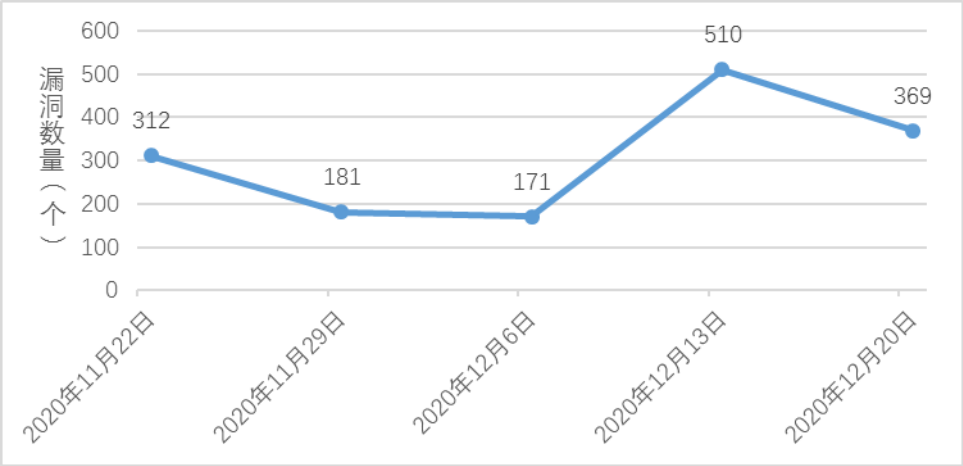

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Apple 公司新增漏洞最多，有 44 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	Apple	44	11.92%
2	IBM	18	4.88%
3	Docker	17	4.61%
4	Siemens	16	3.53%
5	Schneider Electric	17	3.33%

本周国内厂商漏洞 14 个，华为公司漏洞数量最多，有 5 个。国内厂商漏洞整体修复率为 78.57%。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，跨站脚本类的安全漏洞占比最大，达到 10.03%。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	跨站脚本	37	10.03%
2	访问控制错误	29	7.86%
3	输入验证错误	25	6.78%
4	缓冲区错误	24	6.50%
5	代码问题	24	6.50%
6	授权问题	22	5.96%
7	信息泄露	16	4.34%
8	SQL 注入	11	2.98%
9	跨站请求伪造	10	2.71%
10	资源管理错误	6	1.63%
11	权限许可和访问控制问题	6	1.63%
12	路径遍历	5	1.36%
13	信任管理问题	5	1.36%
14	操作系统命令注入	4	1.08%
15	命令注入	4	1.08%
16	注入	3	0.81%
17	代码注入	1	0.27%
18	加密问题	1	0.27%
19	处理逻辑错误	1	0.27%
20	默认配置问题	1	0.27%
21	其他	134	36.31%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 67 个，高危漏洞 111 个，中危漏洞 178 个，低危漏洞 13 个。相应修复率分别为 41.79%、92.79%、88.20%和 100.00%。根据补丁信息统计，合计 301 个漏洞已有修复补丁发布，整体修复率为 81.57%。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	67	28	41.79%
2	高危	111	103	92.79%
3	中危	178	157	88.20%
4	低危	13	13	100.00%
合计		369	301	81.57%

（四） 本周重要漏洞实例

本期重要漏洞实例如表 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	授权问题	CNNVD-202012-1257	Apache 基金会	Apache TomEE 授权问题漏洞	是	超危
2	输入验证错误	CNNVD-202012-1055	Apple	Apple Macos Server 输入验证错误漏洞	是	高危
3	其他	CNNVD-202012-1163	Mozilla 基金会	Mozilla Firefox 安全漏洞	是	高危

1. Apache TomEE 授权问题漏洞（CNNVD-202012-1257）

Apache TomEE 是美国阿帕奇软件（Apache）基金会的一款轻量级的 Java EE 应用程序服务器。

Apache TomEE 存在安全漏洞，该漏洞源于使用嵌入式 ActiveMQ 代理，并且代理配置错误，在 TCP 端口 1099 上打开 JMX 端口，且该端口不包含身份验证。以下产品及版本受到影响：Apache TomEE 8.0.0-M1 版本至 8.0.3 版本，7.1.0 版本至 7.1.3 版本，7.0.0-M1 版本至 7.0.8 版本，1.0.0 版本至 1.7.5 版本。

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.html/ref088c4732e1a8dd0bbbb96e13ffafcfe65f984238ffa55f438d78fe%40%3Cdev.tomee.apache.org%3E

2. Apple Macos Server 输入验证错误漏洞（CNNVD-202012-1055）

Apple Macos Server 是美国 Apple 公司的一款服务端版本的操作系统。

macOS Server 5.11 之前版本存在输入验证错误漏洞，该漏洞源于处理恶意制作的 URL 可能导致开放重定向或跨站点脚本描述。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.apple.com/zh-cn/HT211932

3. Mozilla Firefox 安全漏洞（CNNVD-202012-1163）

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。

Mozilla Firefox 中存在安全漏洞。目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.mozilla.org/en-US/security/advisories/mfsa2

020-54/

二、接报漏洞情况

本周 CNNVD 接报漏洞 12509 个，其中信息技术产品漏洞（通用型漏洞）27 个，网络信息系统漏洞（事件型漏洞）12482 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1.	上海斗象信息科技有限公司	6136
2.	网神信息技术（北京）股份有限公司	5355
3.	河南听潮盛世信息技术有限公司	604
4.	北京奇虎科技有限公司	208
5.	山东华鲁科技发展股份有限公司	95
6.	北京天地和兴科技有限公司	29
7.	杭州海康威视数字技术股份有限公司	18
8.	新疆海狼科技有限公司	12
9.	河南听潮盛世信息科技有限公司	12
10.	北京数字观星科技有限公司	10
11.	山东云天安全技术有限公司	10
12.	杭州默安科技有限公司	7
13.	杭州美创科技有限公司	4
14.	苏州极光无限信息技术有限公司	3
15.	北京市星阑科技有限公司	2
16.	北京智游网安科技有限公司	1
17.	博智安全科技股份有限公司	1
18.	广东东福信息技术有限公司	1

19.	恒安嘉新（北京）科技股份公司	1
报送总计		12509

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 60 份。

	报送单位	预警总量
1	深信服科技股份有限公司	16
2	杭州迪普科技股份有限公司	15
3	北京知道创宇信息技术股份有限公司	5
4	北京启明星辰信息安全技术有限公司	5
5	北京中测安华科技有限公司	3
6	北京奇虎科技有限公司	3
7	北京华云安信息技术有限公司	3
8	新华三技术有限公司	3
9	网神信息技术（北京）股份有限公司	2
10	北京山石网科信息技术有限公司	2
11	北京天融信网络安全技术有限公司	1
12	北京华顺信安科技有限公司	1
13	浪潮电子信息产业股份有限公司	1
报送总计		60