

# 信息安全漏洞周报

(2021 年第 1 期 总第 555 期)

信息安全测评中心

2020 年 1 月 3 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 12 月 28 日至 2021 年 1 月 3 日）安全漏洞情况如下：

## 公开漏洞情况

本周 CNNVD 采集安全漏洞 347 个，与上周（188 个）相比增加了 84.57%。

## 接报漏洞情况

本周 CNNVD 接报漏洞 4001 个，其中信息技术产品漏洞（通用型漏洞）20 个，网络信息系统漏洞（事件型漏洞）3981 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 347 个，漏洞新增数量有所上升。从厂商分布来看 Mozilla 基金会新增漏洞最多，有 83 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 18.73%。新增漏洞中，超危漏洞 31 个，高危漏洞 68 个，中危漏洞 247 个，低危漏洞 1 个。相应修复率分别为 80.65%、94.12%、78.14%和 100.00%。根据补丁信息统计，合计 283 个漏洞已有修复补丁发布，整体修复率为 81.56%。

### （一）安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 347 与上周（188 个）相比增多了 84.57%。

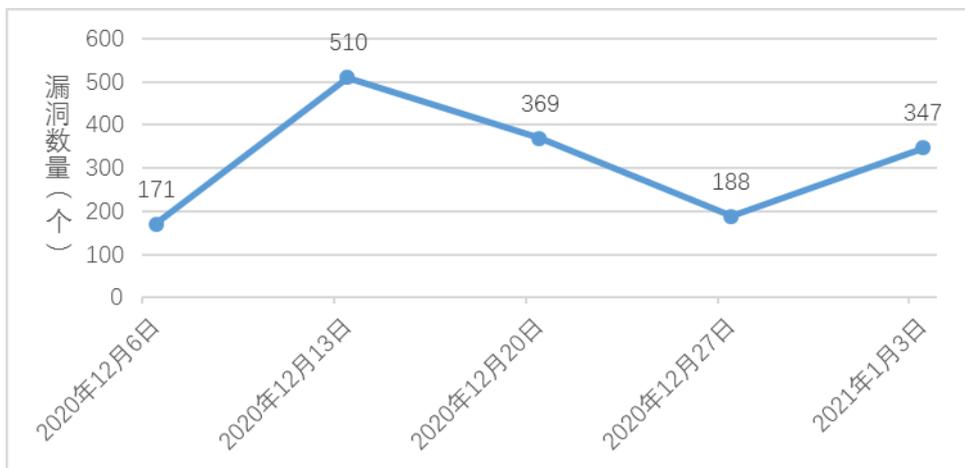


图 1 近五周漏洞新增数量统计图

### （二）安全漏洞分布情况

从厂商分布来看，Mozilla 基金会新增漏洞最多，有 83 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	Mozilla 基金会	83	23.92%
2	NETGEAR	66	19.02%
3	WordPress 基金会	16	4.61%
4	Zammad	11	3.17%
5	Drupal 社区	10	2.88%

本周国内厂商漏洞 25 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 91.30%。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 18.73%。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	65	18.73%
2	输入验证错误	16	4.61%
3	命令注入	13	3.75%
4	缓冲区错误	11	3.17%
5	代码问题	10	2.88%
6	SQL 注入	10	2.88%
7	跨站请求伪造	7	2.02%
8	信息泄露	6	1.73%
9	授权问题	4	1.15%
10	资源管理错误	4	1.15%
11	访问控制错误	3	0.86%
12	路径遍历	3	0.86%
13	权限许可和访问控制问题	3	0.86%
14	信任管理问题	2	0.58%
15	代码注入	2	0.58%
16	数据伪造问题	1	0.29%
17	加密问题	1	0.29%
18	操作系统命令注入	1	0.29%
19	后置链接	1	0.29%
20	处理逻辑错误	1	0.29%
21	默认配置问题	1	0.29%

22	其他	137	39.48%
----	----	-----	--------

### (三) 安全漏洞危害等级与修复情况

本周共发布超危漏洞 31 个，高危漏洞 68 个，中危漏洞 247 个，低危漏洞 1 个。相应修复率分别为 80.65%、94.12%、78.14% 和 100.00%。根据补丁信息统计，合计 283 个漏洞已有修复补丁发布，整体修复率为 81.56%。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	31	25	80.65%
2	高危	68	64	94.12%
3	中危	247	193	78.14%
4	低危	1	1	100.00%
合计		347	283	81.56%

### (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	其他	CNNVD-202012-1889	Wordpress 基金会	WordPress Quiz and Survey Master plugin 安全漏洞	是	超危
2	跨站请求伪造	CNNVD-202012-1752	Netgear	多款 Netgear 产品跨站请求伪造漏洞	是	高危
3	其他	CNNVD-202012-1777	Apache 基金会	Apache Accumulo 安全漏洞	是	高危

#### 1. WordPress Quiz and Survey Master plugin 安全漏洞

(CNNVD-202012-1889)

WordPress 是 WordPress 基金会的一套使用 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 Quiz and Survey Master plugin 是 WordPress 中的一个插件。

Quiz and Survey Master plugin before 7.0.1 for WordPress 存在安全漏洞，攻击者可利用该漏洞上传任意文件并实现远程代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://www.wordfence.com/blog/2020/08/critical-vulnerabilities-patched-in-quiz-and-survey-master-plugin/>

## 2. 多款 Netgear 产品跨站请求伪造漏洞（CNNVD-202012-1752）

Netgear GS716Tv3 和 Netgear GS724Tv4 都是美国 Netgear 公司的一款交换机。

多款 Netgear devices 存在跨站请求伪造漏洞，以下产品及版本受到影响：GS716Tv3 before 6.3.1.36 and GS724Tv4 before 6.3.1.36。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

<https://kb.netgear.com/000062721/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-Smart-Managed-Pro-Switches-PSV-2020-0368>

## 3. Apache Accumulo 安全漏洞（CNNVD-202012-1777）

Apache Accumulo 是 Apache 基金会的一个可靠的、可伸缩的、

高性能的排序分布式的 Key-Value 存储应用。

Apache Accumulo 1.5.0 版本至 1.10.0 版本，2.0.0 版本存在安全漏洞，该漏洞源于经过身份验证的用户执行某些管理操作之前，没有正确地检查一些策略实施函数的返回值。

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/rf8c1a787b6951d3dacb9ec58f0bf1633790c91f54ff10c6f8ff9d8ed%40%3Cuser.apache.org%3E>

## 二、接报漏洞情况

本周 CNNVD 接报漏洞 4001 个，其中信息技术产品漏洞（通用型漏洞）20 个，网络信息系统漏洞（事件型漏洞）3981 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	网神信息技术（北京）股份有限公司	3230
2	上海斗象信息科技有限公司	426
3	河南听潮盛世信息科技有限公司	121
4	西安交大捷普网络科技有限公司	51
5	北京天地和兴科技有限公司	45
6	北京山石网科信息技术有限公司	36
7	山东华鲁科技发展股份有限公司	33
8	山东新潮信息技术有限公司	25
9	山东云天安全技术有限公司	9
10	北京网御星云信息技术有限公司	6

11	博智安全科技股份有限公司	5
12	浙江大华技术股份有限公司	5
13	杭州美创科技有限公司	4
14	恒安嘉新(北京)科技股份公司	4
15	安徽长泰信息安全服务有限公司	1
报送总计		4001

### 三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 64 份。

序号	报送单位	预警总量
1	内蒙古奥创科技有限公司	19
2	杭州迪普科技股份有限公司	14
3	深信服科技股份有限公司	10
4	北京山石网科信息技术有限公司	4
5	北京华云安信息技术有限公司	3
6	北京华顺信安科技有限公司	3
7	北京奇虎科技有限公司	2
8	北京中测安华科技有限公司	2
9	新华三技术有限公司	2
10	北京启明星辰信息安全技术有限公司	1
11	北京知道创宇信息技术股份有限公司	1
12	杭州安恒信息技术股份有限公司	1
13	浪潮电子信息产业股份有限公司	1
14	上海斗象信息科技有限公司	1

报送总计	64
------	----