信息安全漏洞周报

（2021 年第 6 期 总第 560 期）

信息安全测评中心　　2020 年 2 月 7 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2021 年 2 月 1 日至 2021 年 2 月 7 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 474 个，与上周（326 个）相比增加了 45.40%。

接报漏洞情况

本周 CNNVD 接报漏洞 2227 个，其中信息技术产品漏洞（通用型漏洞）99 个，网络信息系统漏洞（事件型漏洞）2128 个。

重大漏洞预警

Sonicwall SMA100 SQL 注入漏洞（CNNVD-202102-394）：成功利用漏洞的攻击者可以在未授权的情况下远程控制目标设备。Sonic SMA 10.2.0.5 之前的版本均受漏洞影响。目前，SonicWall 官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，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 474 个，漏洞新增数量有所上升。从厂商分布来看苹果公司新增漏洞最多，有 64 个；从漏洞类型来看，访问控制错误类的安全漏洞占比最大，达到 8.23%。新增漏洞中，超危漏洞 54 个，高危漏洞 158 个，中危漏洞 254 个，低危漏洞 8 个。相应修复率分别为 72.22%、94.94%、94.88%和 100.00%。根据补丁信息统计，合计 438 个漏洞已有修复补丁发布，整体修复率为 92.41%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 474 与上周（326 个）相比增多了 45.40%。

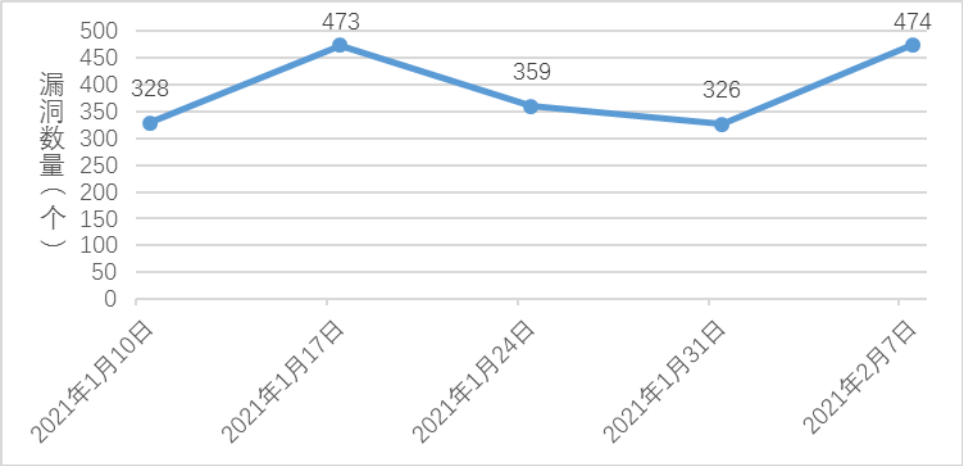

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，苹果公司新增漏洞最多，有 64 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	苹果	64	13.50%
2	思科	56	11.81%
3	谷歌	50	10.55%
4	Qualcomm	29	6.12%
5	JetBrains	26	5.49%

本周国内厂商漏洞 24 个，华为公司漏洞数量最多，有 15 个。国内厂商漏洞整体修复率为 75.00%。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，访问控制错误类的安全漏洞占比最大，达到 8.23%。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	访问控制错误	39	8.23%
2	缓冲区错误	36	7.59%
3	信息泄露	29	6.12%
4	资源管理错误	29	6.12%
5	输入验证错误	26	5.49%
6	跨站脚本	23	4.85%
7	代码问题	17	3.59%
8	授权问题	17	3.59%
9	SQL 注入	13	2.74%
10	命令注入	10	2.11%
11	路径遍历	7	1.48%
12	跨站请求伪造	6	1.27%
13	操作系统命令注入	5	1.05%
14	注入	5	1.05%
15	加密问题	3	0.63%
16	权限许可和访问控制问题	2	0.42%
17	信任管理问题	2	0.42%
18	数据伪造问题	2	0.42%
19	数字错误	2	0.42%
20	代码注入	1	0.21%
21	安全特征问题	1	0.21%

22	其他	198	41.77%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 54 个，高危漏洞 158 个，中危漏洞 254 个，低危漏洞 8 个。相应修复率分别为 72.22%、94.94%、94.88%和 100.00%。根据补丁信息统计，合计 438 个漏洞已有修复补丁发布，整体修复率为 92.41%。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	54	39	72.22%
2	高危	158	150	94.94%
3	中危	254	241	94.88%
4	低危	8	8	100.00%
合计		474	438	92.41%

（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	SQL 注入	CNNVD-202102-394	Sonicwall	Sonicwall SMA100 SQL 注入漏洞	是	超危
2	其他	CNNVD-202102-065	苹果	Apple Safari WebKit 安全漏洞	是	高危
3	其他	CNNVD-202102-271	谷歌	Google Chrome 安全漏洞	是	高危

1. Sonicwall SMA100 SQL 注入漏洞（CNNVD-202102-394）

Sonicwall SMA100 是美国 Sonicwall 公司的一款安全访问网关设备。

SonicWall SSLVPN SMA100 product 存在 SQL 注入漏洞，该漏洞允许远程未经身份验证的攻击者执行 SQL 查询访问用户名密码和其他会话相关信息。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

2. Apple Safari WebKit 安全漏洞（CNNVD-202102-065）

Apple Safari 是美国苹果（Apple）公司的一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。

Safari 14.0.3 WebKit 存在安全漏洞，该漏洞源于恶意制作的 web 内容可能导致任意代码执行。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://support.apple.com/en-us/HT212146

3. Google Chrome 安全漏洞（CNNVD-202102-271）

Google Chromium 是美国谷歌（Google）的一款开源的 Web 浏览器。

Google Chromium 存在安全漏洞，该漏洞源于“扩展”中的堆缓冲区溢出。以下产品和版本受到影响：Microsoft Edge (Chromium-based)。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://chromereleases.googleblog.com/2021/02/stable-channel-update-for-desktop.html

二、接报漏洞情况

本周 CNNVD 接报漏洞 2227 个，其中信息技术产品漏洞（通用型漏洞）99 个，网络信息系统漏洞（事件型漏洞）2128 个。

表 5 本周漏洞报送情况

序号	报送单位	漏洞总量
1	上海斗像信息科技有限公司	1327
2	网神信息技术（北京）股份有限公司	685
3	北京天地和兴科技有限公司	49
4	北京启明星辰信息安全技术有限公司	30
5	北京数字观星科技有限公司	21
6	山东华鲁科技发展股份有限公司	15
7	任子行信息技术有限公司	13
8	南京众智维信息科技有限公司	10
9	北京天融信网络安全技术有限公司	8
10	北京梆梆安全科技有限公司	8
11	山东云天安全技术有限公司	8
12	绿盟科技集团股份有限公司安全研究部	7
13	北京圣博润高新技术股份有限公司	6
14	广州竞远安全技术股份有限公司	6
15	北京机沃科技有限公司	4
16	深信服科技股份有限公司	4
17	个人	3
18	中兴通讯	3
19	北京威努特技术有限公司	3

20	博智安全科技股份有限公司	3
21	恒安嘉新（北京）科技股份公司	3
22	浪潮电子信息产业股份有限公司	3
23	深圳市魔方安全科技有限公司	2
24	北京惠而特科技有限公司	1
25	北京时代新威信息技术有限公司	1
26	北京智游网安科技有限公司	1
27	华为未然实验室	1
28	北京山石网科信息技术有限公司	1
29	海南神州希望网络有限公司	1
报送总计		2227

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 102 份。

序号	报送单位	预警总量
1	深信服科技股份有限公司	22
2	杭州迪普科技股份有限公司	13
3	北京启明星辰信息安全技术有限公司	10
4	北京华云安信息技术有限公司	7
5	北京华顺信安科技有限公司	6
6	网神信息技术（北京）股份有限公司	5
7	北京知道创宇信息技术股份有限公司	5
8	北京山石网科信息技术有限公司	5
9	北京奇虎科技有限公司	5

10	博智安全科技股份有限公司	4
11	浪潮电子信息产业股份有限公司	3
12	任子行网络技术股份有限公司	3
13	新华三技术有限公司	3
14	内蒙古洞明科技有限公司	2
15	北京天融信网络安全技术有限公司	2
16	北京中测安华科技有限公司	2
17	杭州安恒信息技术股份有限公司	2
18	北京安天网络安全技术有限公司	1
19	内蒙古奥创科技有限公司	1
20	远江盛邦(北京)网络安全科技股份有限公司	1
报送总计		102

四、重大漏洞预警

Sonicwall SMA100 SQL 注入漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Sonicwall SMA100 SQL 注入漏洞（CNNVD-202102-394、CVE-2021-20016）情况的报送。成功利用漏洞的攻击者可以在未授权的情况下远程控制目标设备。Sonic SMA 10.2.0.5 之前的版本均受漏洞影响。目前，SonicWall 官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

.漏洞介绍

Sonicwall SMA100 是美国 Sonicwall 公司的一款安全访问网关设备。SonicWall SSLVPN SMA100 product 存在 SQL 注入漏洞，该漏洞允许远程未经身份验证的攻击者执行 SQL 查询访问用户名密码和其他会话相关信息，最终完全控制目标设备。

.危害影响

成功利用漏洞的攻击者可以在未授权的情况下远程控制目标设备。Sonic SMA 10.2.0.5 之前的版本均受漏洞影响。

.修复建议

目前，SonicWall 官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。官方链接如下：

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001