信息安全漏洞周报

（2021 年第 2 期 总第 556 期）

信息安全测评中心　　2020 年 1 月 10 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2021 年 1 月 4 日至 2021 年 1 月 10 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 328 个，与上周（347 个）相比减少了 5.48%。

接报漏洞情况

本周 CNNVD 接报漏洞 6653 个，其中信息技术产品漏洞（通用型漏洞）123 个，网络信息系统漏洞（事件型漏洞）6530 个。

重大漏洞预警

Fortinet 多个安全漏洞预警：其中包括了 FortiGate 安全漏洞（CNNVD-202101-353、CVE-2020-29010）、Fortinet FortiWeb 安全漏洞（CNNVD-202101-356、CVE-2020-29019）等 6 个安全漏洞。成功利用漏洞的攻击者，可通过构造恶意数据远程执行命令，读取内存中的敏感信息等。Fortinet 多个产品及版本受漏洞影响。目前，Fortinet 官方已经发布了版本更新修复了漏洞，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 328 个，漏洞新增数量有所下降。从厂商分布来看 IBM 公司新增漏洞最多，有 38 个；从漏洞类型来看，信息泄露类的安全漏洞占比最大，达到 10.67%。新增漏洞中，超危漏洞 50 个，高危漏洞 81 个，中危漏洞 192 个，低危漏洞 5 个。相应修复率分别为 88.00%、85.19%、91.15%和 100.00%。根据补丁信息统计，合计 293 个漏洞已有修复补丁发布，整体修复率为 89.33%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 328 个，与上周（347 个）相比减少了 5.48%。

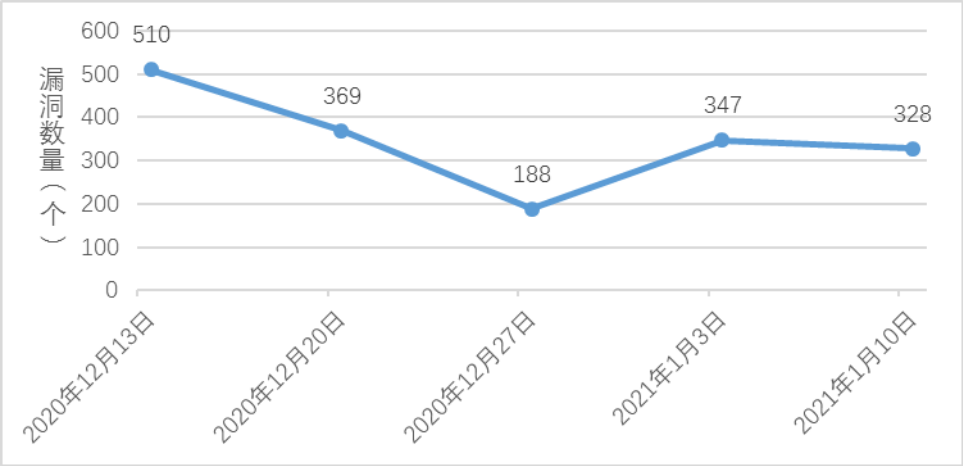

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，IBM 公司新增漏洞最多，有 38 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	IBM	38	11.59%
2	Google	36	10.98%
3	Qualcomm	24	7.32%
4	NVIDIA	16	4.88%
5	Dell	14	4.27%

本周国内厂商漏洞 26 个，福昕公司漏洞数量最多，有 8 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，信息泄露类的安全漏洞占比最大，达到 10.67%。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	信息泄露	35	10.67%
2	跨站脚本	30	9.15%
3	代码问题	28	8.54%
4	缓冲区错误	25	7.62%
5	输入验证错误	22	6.71%
6	资源管理错误	15	4.57%
7	访问控制错误	13	3.96%
8	路径遍历	10	3.05%
9	授权问题	9	2.74%
10	竞争条件问题	8	2.44%
11	注入	7	2.13%
12	SQL 注入	7	2.13%
13	跨站请求伪造	6	1.83%
14	命令注入	3	0.91%
15	加密问题	2	0.61%
16	操作系统命令注入	2	0.61%
17	代码注入	1	0.30%
18	处理逻辑错误	1	0.30%
19	环境问题	1	0.30%
20	日志信息泄露	1	0.30%
21	其他	102	31.10%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 50 个，高危漏洞 81 个，中危漏洞 192 个，低危漏洞 5 个。相应修复率分别为 88.00%、85.19%、91.15%和 100.00%。根据补丁信息统计，合计 293 个漏洞已有修复补丁发布，整体修复率为 89.33%。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	50	44	88.00%
2	高危	81	69	85.19%
3	中危	192	175	91.15%
4	低危	5	5	100.00%
合计		328	293	89.33%

（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-202101-037	Dell	Dell Wyse ThinOS 授权问题漏洞	是	超危
2	其他	CNNVD-202101-276	Linux 基金会	Linux kernel 安全漏洞	是	高危
3	缓冲区错误	CNNVD-202101-384	Google	Google Chrome 缓冲区错误漏洞	是	高危

1. Dell Wyse ThinOS 授权问题漏洞（CNNVD-202101-037）

Dell Wyse ThinOS 是美国戴尔（Dell）公司的一款用于 Dell 服务器的专用操作系统。

Dell Wyse ThinOS 8.6 and prior versions 存在安全漏洞，未

经身份验证的远程攻击者可利用该漏洞访问可写文件并操纵任何目标特定站点的配置。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.dell.com/support/kbdoc/en-us/000180768/dsa-2020-281

2. Linux kernel 安全漏洞（CNNVD-202101-276）

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。

Linux kernel through 5.10.4 存在安全漏洞，该漏洞允许远程攻击者通过一个长 SSID 值执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://github.com/torvalds/linux/commit/5c455c5ab332773464d02ba17015acdca198f03d

3. Google Chrome 缓冲区错误漏洞（CNNVD-202101-384）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。

Google Chrome 87.0.4280.141之前版本中存在缓冲区错误漏洞，攻击者可利用该漏洞执行任意代码。

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/2021/01/stable-channel-update-for-desktop.html

二、接报漏洞情况

本周 CNNVD 接报漏洞 6653 个，其中信息技术产品漏洞（通用型

漏洞）123 个，网络信息系统漏洞（事件型漏洞）6530 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	4013
2	网神信息技术（北京）股份有限公司	1638
3	北京山石网科信息技术有限公司	493
4	北京华云安信息技术有限公司	117
5	北京天地和兴科技有限公司	85
6	山东华鲁科技发展股份有限公司	55
7	北京启明星辰信息安全技术有限公司	52
8	河南听潮盛世信息技术有限公司	51
9	广州锦行网络科技有限公司	20
10	星云博创摘星实验室	20
11	北京数字观星科技有限公司	16
12	中国电信集团系统集成有限责任公司	14
13	恒安嘉新(北京)科技股份公司	10
14	山东云天安全技术有限公司	10
15	博智安全科技股份有限公司	9
16	上海安识网络科技有限公司	8
17	浪潮电子信息产业股份有限公司	5
18	中国科学院软件研究所	5
19	北京网御星云信息技术有限公司	4
20	深信服科技股份有限公司	4
21	中兴通讯	4

22	安全邦（北京）信息技术有限公司	3
23	杭州安恒信息技术股份有限公司	3
24	浙江宇视科技有限公司	3
25	北京智游网安科技有限公司	2
26	亚信科技（成都）有限公司	2
27	个人	2
28	北京安华金和科技有限公司	1
29	北京市星阑科技有限公司	1
30	北京天融信网络安全技术有限公司	1
31	北京威努特技术有限公司	1
32	国防科技大学	1
报送总计		6653

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 75 份。

序号	报送单位	预警总量
1	杭州迪普科技股份有限公司	16
2	深信服科技股份有限公司	11
3	北京山石网科信息技术有限公司	5
4	北京华顺信安科技有限公司	5
5	浪潮电子信息产业股份有限公司	5
6	北京华云安信息技术有限公司	5
7	北京启明星辰信息安全技术有限公司	5
8	内蒙古奥创科技有限公司	4

9	北京奇虎科技有限公司	4
10	网神信息技术（北京）股份有限公司	3
11	北京中测安华科技有限公司	3
12	新华三技术有限公司	2
13	杭州安恒信息技术股份有限公司	2
14	内蒙古洞明科技有限公司	2
15	北京知道创宇信息技术股份有限公司	1
16	上海斗象信息科技有限公司	1
17	远江盛邦(北京)网络安全科技股份有限公司	1
报送总计		75

四、重大漏洞预警

Fortinet 多个安全漏洞的预警

近日，国家信息安全漏洞库（CNNVD）收到关于 Fortinet 多个安全漏洞的通报，其中包括 FortiGate 安全漏洞（CNNVD-202101-353、CVE-2020-29010 ）、Fortinet FortiWeb 安全漏洞（CNNVD-202101-356、CVE-2020-29019）等 6 个安全漏洞。成功利用漏洞的攻击者，可通过构造恶意数据远程执行命令，读取内存中的敏感信息等。Fortinet 多个产品及版本受漏洞影响。目前，Fortinet 官方已经发布了版本更新修复了漏洞，建议用户及时确认产品版本，尽快采取修补措施。

.漏洞介绍

Fortinet FortiGate 、 Fortinet FortiWeb 、 Fortinet FortiDeceptor 等都是美国飞塔（Fortinet）公司的产品，其中 Fortinet FortiGate 是一套网络安全平台。Fortinet FortiWeb 是一款 Web 应用层防火墙。Fortinet FortiDeceptor 是一款网络威胁检测平台。

1 、 Fortinet FortiGate 安 全 漏 洞 （ CNNVD-202101-353 、 CVE-2020-29010）：FortiGate 存在安全漏洞，攻击者可利用该漏洞通过 Events Log Entries 绕过对数据的访问限制，以获取敏感信息。以下产品及版本受到影响：FortiWeb 6.3.5 及以下版本， FortiWeb 6.2.3 及以下版本。

2 、 Fortinet FortiWeb SQL 注 入 漏 洞 （ CNNVD-202101-361 、 CVE-2020-29015）：FortiWeb 的用户界面存在 SQL 注入漏洞，该漏洞源于允许未经身份验证的远程攻击者发送包含精心设计的 Authorization 标头的请求来执行 SQL 语句。以下产品及版本受到影响：FortiWeb 6.3.7 及以下版本，FortiWeb 6.2.3 及以下版本。

3、Fortinet FortiWeb 缓冲区错误漏洞（CNNVD-202101-358、CVE-2020-29016）：FortiWeb 存在缓冲区错误漏洞，该漏洞允许未经身份验证的远程攻击者覆盖堆栈的内容。并执行任意代码。以下产品及版本受到影响：FortiWeb 6.3.5 及以下版本，FortiWeb 6.2.3 及以下版本。

4、Fortinet FortiDeceptor 安全漏洞（CNNVD-202101-363、CVE-2020-29017）：FortiDeceptor 存在安全漏洞，该漏洞允许远程用户在目标系统上执行任意 shell 命令。以下产品及版本受到影响：FortiDeceptor 3.0.0, 3.0.1, 3.1.0。

5、Fortinet FortiWeb 安全漏洞（CNNVD-202101-360、CVE-2020-29018）：Fortinet FortiWeb 存在安全漏洞，该漏洞允许远程用户访问敏感信息。以下产品及版本受到影响：Fortinet FortiWeb 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5。

6、Fortinet FortiWeb 安全漏洞（CNNVD-202101-356、CVE-2020-29019）：Fortinet FortiWeb 存在安全漏洞，该漏洞允许远程攻击者执行拒绝服务(DoS)攻击。以下产品及版本受到影响：Fortinet FortiWeb 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7。

.修复建议

目前，Fortinet 官方已经发布了版本更新修复了漏洞，建议用户及时确认产品版本，尽快采取修补措施。Fortinet 官方更新链接如下：

序号	漏洞名称	官方链接
1	Fortinet FortiGate 安全漏洞（CNNVD-202101-353、CVE-2020-29010）	https://www.fortiguard.com/psirt/FG-IR-20-103
2	Fortinet FortiWeb SQL 注入漏洞	https://www.fortiguard.com/psirt/%20

	（CNNVD-202101-361、CVE-2020-29015）	FG-IR-20-124
3	Fortinet FortiWeb 缓冲区错误漏洞（CNNVD-202101-358、CVE-2020-29016）	https://www.fortiguard.com/psirt/FG-IR-20-125
4	Fortinet FortiDeceptor 安全漏洞（CNNVD-202101-363、CVE-2020-29017）	https://www.fortiguard.com/psirt/FG-IR-20-177
5	Fortinet FortiWeb 安全漏洞（CNNVD-202101-360、CVE-2020-29018）	https://www.fortiguard.com/psirt/FG-IR-20-123
6	Fortinet FortiWeb 安全漏洞（CNNVD-202101-356、CVE-2020-29019）	https://www.fortiguard.com/psirt/%20FG-IR-20-126