信息安全漏洞周报

（2020 年第 35 期 总第 539 期）

信息安全测评中心　　2020 年 9 月 6 日

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 08 月 31 日至 2020 年 09 月 06 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 353 个，与上周（264 个）相比增加了 33.71%。

接报漏洞情况

本周 CNNVD 接报漏洞 1274 个，其中信息技术产品漏洞（通用型漏洞）50 个，网络信息系统漏洞（事件型漏洞）1224 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 353 个，漏洞新增数量有所上升。从厂商分布来看 GitLab 公司新增漏洞最多，有 19 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 15.86%。新增漏洞中，超危漏洞 42 个，高危漏洞 91 个，中危漏洞 215 个，低危漏洞 5 个。相应修复率分别为 80.95%、69.23%、70.70%和 100.00%。根据补丁信息统计，合计 254 个漏洞已有修复补丁发布，整体修复率为 71.95%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 353 与上周（264 个）相比增多了 33.71%。

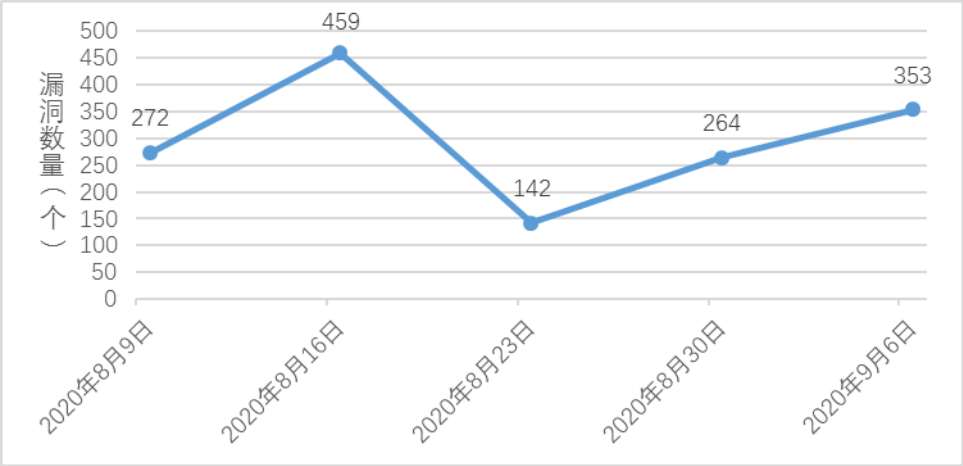

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，GitLab 公司新增漏洞最多，有 19 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	GitLab	19	5.38%
2	IBM	17	4.82%
3	Cisco	17	4.82%
4	CloudBees	14	3.97%
5	Google	13	3.68%

本周国内厂商漏洞 13 个，Huawei 公司漏洞数量最多，有 3 个。国内厂商漏洞整体修复率为 90.91%。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 15.86%。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	56	15.86%
2	SQL 注入	31	8.78%
3	输入验证错误	25	7.08%
4	信息泄露	11	3.12%
5	路径遍历	5	1.42%
6	代码问题	5	1.42%
7	代码注入	5	1.42%
8	跨站请求伪造	4	1.13%
9	缓冲区错误	3	0.85%
10	命令注入	2	0.57%
11	权限许可和访问控制问题	2	0.57%
12	操作系统命令注入	1	0.28%
13	加密问题	1	0.28%
14	访问控制错误	1	0.28%
15	信任管理问题	1	0.28%
16	注入	1	0.28%
17	数据伪造问题	1	0.28%
18	日志信息泄露	1	0.28%
19	后置链接	1	0.28%
20	其他	153	43.34%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 42 个，高危漏洞 91 个，中危漏洞 215 个，低危漏洞 5 个。相应修复率分别为 80.95%、69.23%、70.70%和 100.00%。根据补丁信息统计，合计 254 个漏洞已有修复补丁发布，整体修复率为 71.95%。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	42	34	80.95%
2	高危	91	63	69.23%
3	中危	215	152	70.70%
4	低危	5	5	100.00%
合计		353	254	71.95%

（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-202008-1494	Google	Android 安全漏洞	是	超危
2	跨站请求伪造	CNNVD-202009-028	CloudBees	CloudBees Jenkins CSRF 漏洞	是	高危
3	其他	CNNVD-202009-295	IBM	IBM Aspera Connect 安全漏洞	是	高危

1. Android 安全漏洞（CNNVD-202008-1494）

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。Framework 是其中的一个 Android 框架组件。System 是其中的一个系统组件。Broadcom

Bluetooth 是其中的一个蓝牙组件。Wi-Fi 是其中的一个无线上网组件。USB driver 是其中的一个通用串行总线（USB）驱动程序。VPN 是其中的一个 VPN（虚拟专用网络）组件。Bluetooth 是其中的一个蓝牙组件。Email 是其中的一个电子邮件组件。

Android OS 9 and 10 中的 LG mobile 设备存在安全漏洞，攻击者利用此漏洞可以绕过权限限制。

目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：

https://lgsecurity.lge.com/

2. CloudBees Jenkins CSRF 漏洞（CNNVD-202009-028）

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。LTS 是 CloudBeesJenkins 的一个长期支持版本。

Jenkins database Plugin 1.6 及之前版本存在 CSRF 漏洞，该漏洞源于 WEB 应用未充分验证请求是否来自可信用户。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://vigilance.fr/vulnerabilite/Jenkins-Plugins-multiples-vulnerabilites-33205

3. IBM Aspera Connect 安全漏洞（CNNVD-202009-295）

IBM Aspera 是美国 IBM 公司的一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。

IBM Aspera Connect 3.9.9 版本存在安全漏洞，该漏洞源于动态链接库加载不正确，攻击者可以利用此漏洞诱使受害者打开特制的.DLL 文件，从而执行任意代码。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.ibm.com/support/pages/node/6326537

二、接报漏洞情况

本周 CNNVD 接报漏洞 1274 个，其中信息技术产品漏洞（通用型漏洞）50 个，网络信息系统漏洞（事件型漏洞）1224 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	648
2	网神信息技术（北京）股份有限公司	356
3	内蒙古奥创科技有限公司	94
4	北京奇虎科技有限公司	37
5	杭州海康威视数字技术股份有限公司	36
6	西安交大捷普网络科技有限公司	24
7	北京山石网科信息技术有限公司	11
8	北京数字观星科技有限公司	10
9	美团安全	10
10	湖南匡安网络技术有限公司	8
11	个人	7
12	中国电信集团系统集成有限责任公司	6

13	新华三技术有限公司	5
14	安全邦（北京）信息技术有限公司	5
15	重庆梦之想科技有限公司	4
16	苏州极光无限信息技术有限公司	2
17	上海安识网络科技有限公司	2
18	阿里安全	1
19	安徽长泰信息安全服务有限公司	1
20	北京网御星云信息技术有限公司	1
21	国网山西省电力公司电力科学研究院	1
22	江西神舟信息安全评估中心有限公司	1
23	上海市信息安全测评中心	1
24	深信服科技股份有限公司	1
25	亚信科技（成都）有限公司	1
26	中国电信集团系统集成有限责任公司云计算安全与服务事业部	1
报送总计		1274

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 31 个。

序号	报送单位	漏洞总量
1	杭州迪普科技有限公司	15
2	北京知道创宇信息技术股份有限公司	4
3	北京华云安信息技术有限公司	4
4	北京启明星辰信息安全技术有限公司	2
5	网神信息技术（北京）股份有限公司	1

6	新华三技术有限公司	1
7	杭州安恒信息技术股份有限公司	1
8	深信服科技股份有限公司	1
9	北京山石网科信息技术有限公司	1
10	内蒙古洞明科技有限公司	1
报送总计		31