信息安全漏洞周报

（2020 年第 9 期 总第 513 期）

信息安全测评中心 **2020 年 3 月 9 日**

根据国家信息安全漏洞库（CNNVD）统计，本周（2020 年 3 月 2 日至 2020 年 3 月 8 日）安全漏洞情况如下：

公开漏洞情况

本周 CNNVD 采集安全漏洞 261 个，与上周（215 个）相比增加了 21.40%。

接报漏洞情况

本周 CNNVD 接报漏洞 590 个，其中信息技术产品漏洞（通用型漏洞）26 个，网络信息系统漏洞（事件型漏洞）564 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 261 个，漏洞新增数量有所上升。从厂商分布来看，Qualcomm 公司新增漏洞最多，有 48 个；从漏洞类型来看，缓冲区错误类的安全漏洞占比最大，达到 15.71%。新增漏洞中，本周共发布超危漏洞 44 个，高危漏洞 109 个，中危漏洞 99 个，低危漏洞 9 个。相应修复率分别为 68.18%、82.57%、78.79%和 66.67%。根据补丁信息统计，合计 204 个漏洞已有修复补丁发布，整体修复率为 78.16%。

（一） 安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 261 个，与上周（215 个）相比增加了 21.40%。图 1 为近五周漏洞新增数量统计图。

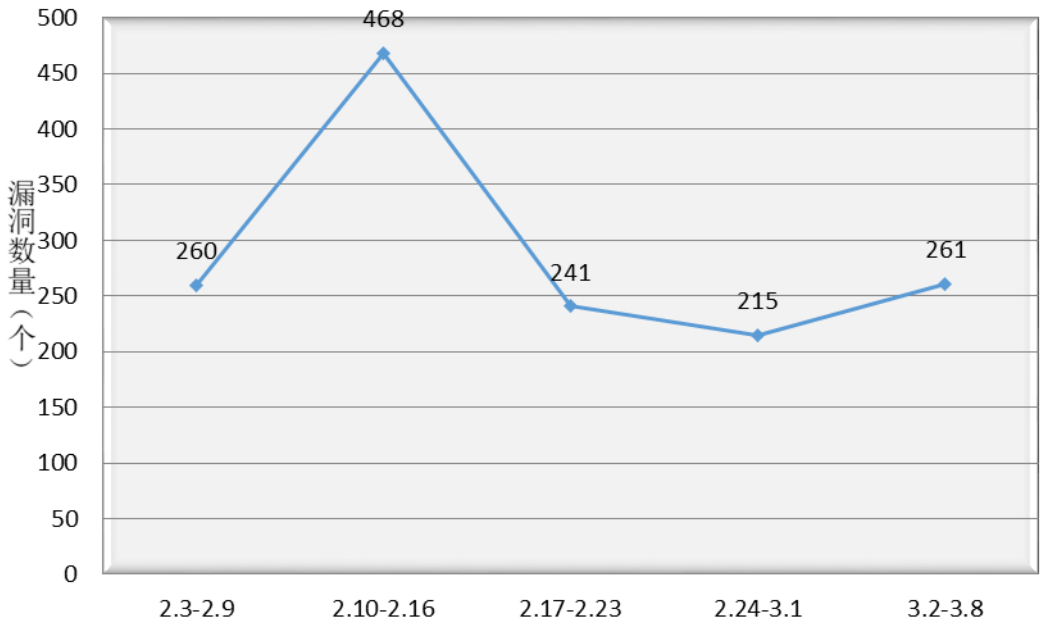

图 1 近五周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，Qualcomm 公司新增漏洞最多，有 48 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	Qualcomm	48	18.39%
2	Google	45	17.24%
3	Cisco	13	4.98%
4	D-Link	13	4.98%
5	Zammad	10	3.83%

本周国内厂商漏洞 17 个，D-Link 公司漏洞数量最多，有 13 个。国内厂商漏洞整体修复率为 58.82%。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，缓冲区错误类的安全漏洞占比最大，达到 15.71%。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	缓冲区错误	41	15.71%
2	跨站脚本	27	10.34%
3	代码问题	14	5.36%
4	输入验证错误	12	4.60%
5	SQL 注入	10	3.83%
6	信息泄露	10	3.83%
7	资源管理错误	10	3.83%
8	授权问题	8	3.07%
9	跨站请求伪造	6	2.30%
10	操作系统命令注入	4	1.53%
11	访问控制错误	4	1.53%
12	注入	4	1.53%
13	后置链接	2	0.77%
14	路径遍历	2	0.77%
15	命令注入	2	0.77%
16	数字错误	2	0.77%
17	安全特征问题	1	0.38%
18	加密问题	1	0.38%

19	竞争条件问题	1	0.38%
20	日志信息泄露	1	0.38%
21	数据伪造问题	1	0.38%
22	信任管理问题	1	0.38%
23	其他	97	37.16%

（三） 安全漏洞危害等级与修复情况

本周共发布超危漏洞 44 个，高危漏洞 109 个，中危漏洞 99 个，低危漏洞 9 个。相应修复率分别为 68.18%、82.57%、78.79%和 66.67%。根据补丁信息统计，合计 204 个漏洞已有修复补丁发布，整体修复率为 78.16%。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	44	30	68.18%
2	高危	109	90	82.57%
3	中危	99	78	78.79%
4	低危	9	6	66.67%
合计		261	204	78.16%

（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	缓冲区错误	CNNVD-202003-086	Qualcomm	多款 Qualcomm 产品 WLAN 缓冲区错误漏洞	是	超危
2	操作系统命令注入	CNNVD-202003-201	D-Link	D-Link DWL-2600AP 操作系统命令注入漏洞	是	高危
3	跨站请求伪造	CNNVD-202003-182	Cisco	Cisco Prime Network Registrar 跨站请求伪造漏洞	是	高危

1. 多款 Qualcomm 产品 WLAN 缓冲区错误漏洞（CNNVD-202003-086）

Qualcomm MDM9206 等都是美国高通（Qualcomm）公司的一款中央处理器（CPU）产品。

多款 Qualcomm 产品中的 WLAN 组件存在缓冲区错误漏洞，该漏洞源于程序没有进行正确的边界检查。远程攻击者可利用该漏洞执行任意代码，或导致应用程序崩溃。以下产品及版本受到影响：Qualcomm APQ8009；APQ8017；APQ8053；APQ8096；APQ8098；IPQ8074；MDM9206；MDM9207C；MDM9607；MSM8996；MSM8996AU；MSM8998；QCA6174A；QCA6574AU；QCA8081；QCA9377；QCA9379；QCA9886；QCS605；SDA660；SDA845；SDM630；SDM636；SDM660；SDM670；SDM710；SDM845；SDM850；SM6150；SM7150；SM8150；SXR1130。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://www.qualcomm.com/company/product-security/bulletins/march-2020-bulletin

2. D-Link DWL-2600AP 操作系统命令注入漏洞（CNNVD-202002-1192）

D-Link DWL-2600AP 是中国台湾友讯（D-Link）公司的一款无线接入点设备。

D-Link DWL-2600AP 4.2.0.15 Rev A 版本中存在操作系统命令注入漏洞。攻击者可借助恢复配置功能利用该漏洞执行任意操作系统命令。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10113

3. Cisco Prime Network Registrar 跨站请求伪造漏洞（CNNVD-202003-182）

Cisco Prime Network Registrar（CPNR）是美国思科（Cisco）公司的一款网络注册器产品。该产品提供了动态主机配置协议（DHCP）、域名系统（DNS）和 IP 地址管理（IPAM）等服务。

Cisco CPNR 10.1 之前版本（releases）中基于 Web 的接口存在跨站请求伪造漏洞，该漏洞源于程序没有进行充分的跨站请求伪造保护。远程攻击者可通过诱使用户点击恶意链接利用该漏洞修改设备配置，进而可以编辑或创建任意权限用户的账户。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cpnr-csrf-WWTrDkyL

二、接报漏洞情况

本周 CNNVD 接报漏洞 590 个，其中信息技术产品漏洞（通用型漏洞）26 个，网络信息系统漏洞（事件型漏洞）564 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	226
2	上海斗象信息科技有限公司	152
3	北京华云安信息技术有限公司	139

4	上海安洵信息技术有限公司	18
5	北京圣溥润高新技术服份有限公司	14
6	北京国舜科技股份有限公司	10
7	北京云测信息技术有限公司	10
8	北京数字观星科技有限公司	6
9	成都科来软件有限公司	4
10	中国电信集团系统集成有限责任公司	4
11	北京梆梆安全科技有限公司	3
12	上海安识网络科技有限公司	2
13	北京神州绿盟科技有限公司	1
14	锐捷网络股份有限公司	1
报送总计		590