信息安全漏洞周报

（2019 年第 5 期 总第 459 期）

信息安全测评中心　　2019 年 2 月 10 日

根据国家信息安全漏洞库（CNNVD）统计， 2019 年 1 月 28 日至 2 月 10 日安全漏洞情况如下：

公开漏洞情况

2019 年 1 月 28 日至 2 月 10 日 CNNVD 采集安全漏洞 157 个，与上期（293 个）相比下降了 46.42%。

接报漏洞情况

2019 年 1 月 28 日至 2 月 10 日接报漏洞 1224 个，其中信息技术产品漏洞（通用型漏洞）8 个，网络信息系统漏洞（事件型漏洞）1216 个。

一、公开漏洞情况

根据国家信息安全漏洞库（CNNVD）统计，2019 年 1 月 28 日至 2 月 10 日新增安全漏洞 157 个，漏洞新增数量有所下降。从厂商分布来看，其中谷歌公司新增漏洞最多，共有 29 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 14.74%。新增漏洞中，超危漏洞 1 个，高危漏洞 16 个，中危漏洞 121 个，低危漏洞 19 个。相应修复率分别为 100.00%、87.50%、82.64%以及 63.16%。根据补丁信息统计，合计 127 个漏洞已有修复补丁发布，整体修复率为 80.89%。

截至 2019 年 2 月 10 日，CNNVD 发布漏洞总量已达 121434 个。

（一） 安全漏洞增长数量情况

2019 年 1 月 28 日至 2 月 10 日 CNNVD 采集安全漏洞 157 个，与上期（293 个）相比下降了 46.42%。图 1 为近六周漏洞新增数量统计图。

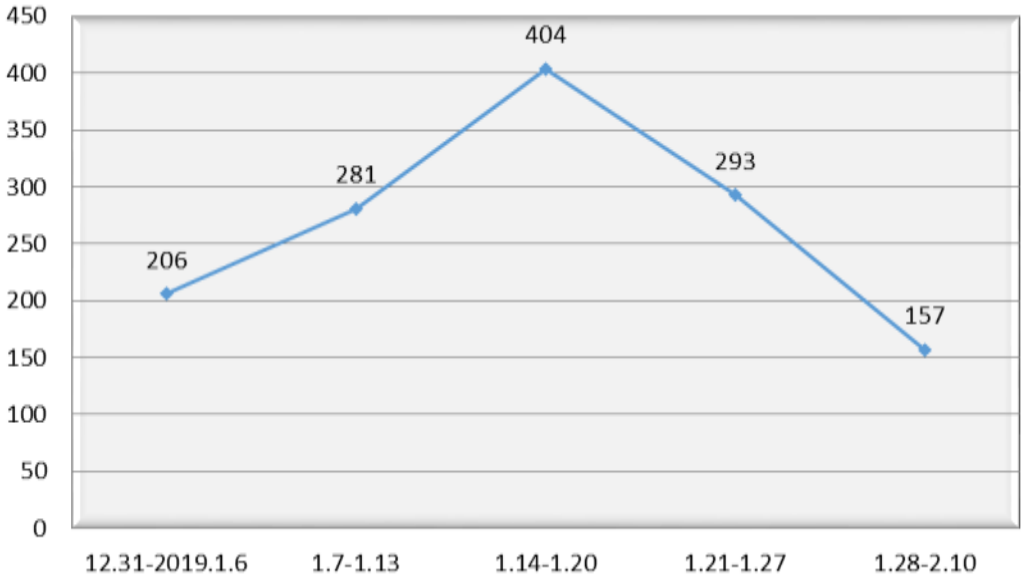

图 1 近六周漏洞新增数量统计图

（二） 安全漏洞分布情况

从厂商分布来看，2019 年 1 月 28 日至 2 月 10 日期间谷歌公司新增漏洞最多，共 29 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	所占比例
1	谷歌	29	18.59%
2	Mozilla	7	4.49%
3	IBM	5	3.21%
4	Phoenix Contact	5	3.21%
5	福昕	4	2.56%

2019 年 1 月 28 日至 2 月 10 日期间，国内厂商漏洞共 8 个，福昕公司漏洞数量最多，共 4 个。国内厂商漏洞整体修复率为 87.50%。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，2019 年 1 月 28 日至 2 月 10 日期间，跨站脚本类的安全漏洞相对占比最大，达到 14.74%。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	所占比例
1	跨站脚本	23	14.74%
2	缓冲区错误	20	12.83%
3	输入验证	5	3.21%
4	跨站请求伪造	4	2.56%
5	SQL 注入	4	2.56%
6	路径遍历	2	1.28%
7	信息泄露	2	1.28%
8	访问控制错误	2	1.28%
9	授权问题	1	0.64%
10	安全特征问题	1	0.64%
11	资源管理错误	1	0.64%

（三） 安全漏洞危害等级与修复情况

2019 年 1 月 28 日至 2 月 10 日，共发布超危漏洞 1 个，高危漏

洞 16 个，中危漏洞 121 个，低危漏洞 19 个。相应修复率分别为 100.00%、87.50%、82.64%以及 63.16%。合计 127 个漏洞已有修复补丁发布，整体修复率为 80.89%。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	修复数量	修复率
1	超危	1	1	100.00%
2	高危	16	14	87.50%
3	中危	121	100	82.64%
4	低危	19	12	63.16%
合计		157	127	80.89%

（四）重要漏洞实例

重要漏洞实例如表 4 所示。

表 4 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-201901-888	研华	Advantech WebAccess/SCADA 授权问题漏洞	是	超危
2	跨站请求伪造	CNNVD-201901-894	Phoenix Contact	Phoenix Contact FL SWITCH 跨站请求伪造漏洞	是	高危
3	缓冲区错误	CNNVD-201901-1034	ACD Systems	ACD Systems Canvas Draw 缓冲区错误漏洞	是	高危

1. Advantech WebAccess/SCADA 授权问题漏洞（CNNVD-201901-888）

Advantech WebAccess/SCADA 是研华（Advantech）公司的一套基于浏览器架构的 SCADA 软件。该软件支持动态图形显示和实时数据控制，并提供远程控制和管理自动化设备的功能。

Advantech WebAccess/SCADA 8.3 版本中存在授权问题漏洞。攻击者可利用该漏洞绕过身份验证，上传恶意数据。

目前厂商已发布升级补丁以修复漏洞，补丁获取链接:

https://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download

2. Phoenix Contact FL SWITCH 跨站请求伪造漏洞（CNNVD-201901-894）

Phoenix Contact FL SWITCH 是德国菲尼克斯电气（Phoenix Contact）集团的一款工业级以太网交换机。

Phoenix Contact FL SWITCH 3xxx 1.35 之前版本、4xxx 1.35 之前版本和 48xx 1.35 之前版本中存在跨站请求伪造漏洞。远程攻击者可通过发送畸形的 HTTP 请求利用该漏洞执行未授权的操作。

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://www.phoenixcontact.com

3. ACD Systems Canvas Draw 缓冲区错误漏洞（CNNVD-201901-1034）

ACD Systems Canvas Draw 是美国 ACD Systems 公司的一款图形编辑工具，它主要用于创建和编辑图像等。

ACD Systems Canvas Draw 5.0.0.28 版本中的 CALS Raster 文件解析功能存在越界写入漏洞。攻击者可借助特制的 CAL 图像利用该漏洞覆盖任意数据，执行代码。

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://www.acdsystems.com/

二、接报漏洞情况

2019 年 1 月 28 日至 2 月 10 日接报漏洞 1224 个，其中信息技术

产品漏洞（通用型漏洞）8 个，网络信息系统漏洞（事件型漏洞）1216 个。

表 5 漏洞报送情况

序号	报送单位	漏洞总量	通用型漏洞	事件型漏洞
1	上海斗象信息科技有限公司	760	0	760
2	网神信息技术（北京）股份有限公司	341	0	341
3	四川虹微技术有限公司	48	0	48
4	中新网络信息安全股份有限公司	21	1	20
5	内蒙古奥创科技有限公司	17	0	17
6	北京圣博润高新技术股份有限公司	12	0	12
7	北京数字观星科技有限公司	11	0	11
8	上海三零卫士信息安全有限公司	4	4	0
9	国发中新（北京）科技发展有限公司	3	0	3
10	安徽锋刃信息科技有限公司	2	2	0
11	河南听潮盛世信息技术有限公司	2	0	2
12	西安交大捷普网络科技有限公司	1	0	1
13	亚信科技（成都）有限公司	1	1	0
14	河南听潮盛世信息技术有限公司	1	0	1
报送总计		1224	8	1216