

信息安全漏洞周报

(2021 年第 8 期 总第 562 期)

信息安全测评中心

2021 年 2 月 21 日

根据国家信息安全漏洞库 (CNNVD) 统计, 本周 (2021 年 2 月 15 日至 2021 年 2 月 21 日) 安全漏洞情况如下:

公开漏洞情况

本周 CNNVD 采集安全漏洞 255 个, 与上周 (553 个) 相比减少了 53.89%。

接报漏洞情况

本周 CNNVD 接报漏洞 1493 个, 其中信息技术产品漏洞 (通用型漏洞) 13 个, 网络信息系统漏洞 (事件型漏洞) 1480 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 255 个，漏洞新增数量有所下降。从厂商分布来看谷歌公司新增漏洞最多，有 9 个；从漏洞类型来看，跨站脚本类的安全漏洞占比最大，达到 9.02%。新增漏洞中，超危漏洞 20 个，高危漏洞 99 个，中危漏洞 127 个，低危漏洞 9 个。相应修复率分别为 80.00%、82.83%、70.87%和 100.00%。根据补丁信息统计，合计 197 个漏洞已有修复补丁发布，整体修复率为 77.25%。

（一）安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 255 与上周（553 个）相比减少了 53.89%。

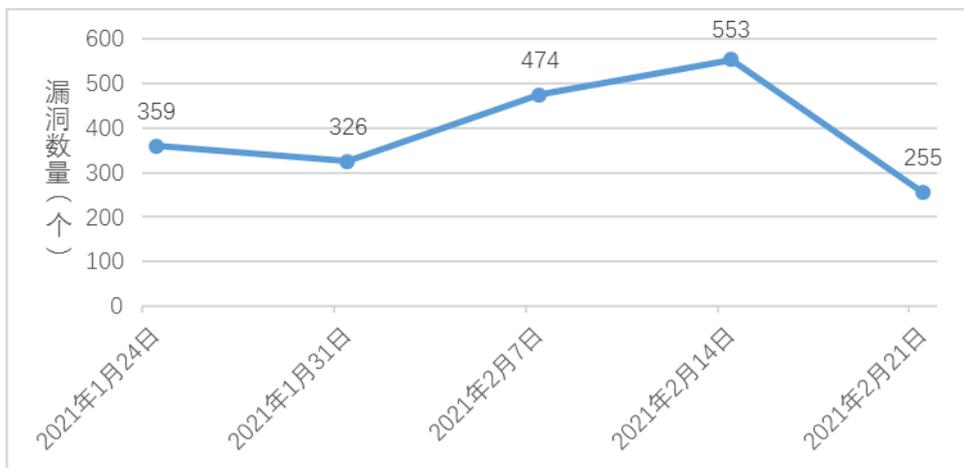


图 1 近五周漏洞新增数量统计图

（二）安全漏洞分布情况

从厂商分布来看，谷歌公司新增漏洞最多，有 9 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 | 谷歌 | 9 | 3.53% |
| 2 | IBM | 6 | 2.35% |
| 3 | Red Hat | 6 | 2.35% |
| 4 | Linux 基金会 | 6 | 2.35% |
| 5 | 西科姆 | 6 | 2.35% |

本周国内厂商漏洞 16 个，研华公司漏洞数量最多，有 6 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，跨站脚本类的安全漏洞占比最大，达到 9.02%。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 | 23 | 9.02% |
| 2 | SQL 注入 | 18 | 7.06% |
| 3 | 缓冲区错误 | 14 | 5.49% |
| 4 | 信息泄露 | 12 | 4.71% |
| 5 | 权限许可和访问控制问题 | 11 | 4.31% |
| 6 | 路径遍历 | 11 | 4.31% |
| 7 | 输入验证错误 | 9 | 3.53% |
| 8 | 访问控制错误 | 7 | 2.75% |
| 9 | 命令注入 | 7 | 2.75% |
| 10 | 操作系统命令注入 | 7 | 2.75% |
| 11 | 代码问题 | 6 | 2.35% |
| 12 | 资源管理错误 | 6 | 2.35% |
| 13 | 跨站请求伪造 | 6 | 2.35% |
| 14 | 注入 | 5 | 1.96% |
| 15 | 授权问题 | 3 | 1.18% |
| 16 | 信任管理问题 | 1 | 0.39% |
| 17 | 代码注入 | 1 | 0.39% |
| 18 | 加密问题 | 1 | 0.39% |
| 19 | 数据伪造问题 | 1 | 0.39% |
| 20 | 其他 | 105 | 41.18% |

（三）安全漏洞危害等级与修复情况

本周共发布超危漏洞 20 个，高危漏洞 99 个，中危漏洞 127 个，低危漏洞 9 个。相应修复率分别为 80.00%、82.83%、70.87%和 100.00%。根据补丁信息统计，合计 197 个漏洞已有修复补丁发布，整体修复率为 77.25%。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 | 20 | 16 | 80.00% |
| 2 | 高危 | 99 | 82 | 82.83% |
| 3 | 中危 | 127 | 90 | 70.87% |
| 4 | 低危 | 9 | 9 | 100.00% |
| 合计 | | 255 | 197 | 77.25% |

（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 | 操作系统命令注入 | CNNVD-202102-1249 | Accellion | Accellion FTA 操作系统命令注入漏洞 | 是 | 超危 |
| 2 | 操作系统命令注入 | CNNVD-202102-1136 | Nagios | Nagios XI 操作系统命令注入漏洞 | 是 | 高危 |
| 3 | 数据伪造问题 | CNNVD-202102-1301 | 思科 | 思科 Cisco AnyConnect Secure Mobility Client 数据伪造问题漏洞 | 是 | 高危 |

1. Accellion FTA 操作系统命令注入漏洞（CNNVD-202102-1249）

Accellion FTA 是美国 Accellion 公司的一个企业内容防火墙。提供了一个防止来自第三方网络风险的数据泄露和违规行为。

Accellion FTA 中存在操作系统命令注入漏洞，该漏洞源于外部输入数据构造操作系统可执行命令过程中，网络系统或产品未正确过滤其中的特殊字符、命令导致。攻击者可利用该漏洞执行非法操作系统命令。

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.accellion.com/products/fta/>

2. Nagios XI 操作系统命令注入漏洞（CNNVD-202102-1136）

Nagios XI 是美国 Nagios 公司的一套 IT 基础设施监控解决方案。该方案支持对应用、服务、操作系统等进行监控和预警。

NagiosXI xi-5.7.5 中存在操作系统命令注入漏洞，该漏洞源于外部输入数据构造可执行命令过程中，网络系统或产品未正确过滤其中的特殊元素。攻击者可利用该漏洞执行非法命令。

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.nagios.com/>

3. 思科 Cisco AnyConnect Secure Mobility Client 数据伪造问题漏洞（CNNVD-202102-1301）

Cisco Anyconnect Secure Mobility Client 是美国思科（Cisco）公司的一款用于安全连接的 VPN 客户端软件。

Cisco AnyConnect Secure Mobility Client 中存在数据伪造问题漏洞，该漏洞源于网络系统或产品未充分验证数据的来源或真实性。攻击者可利用伪造的数据进行攻击。

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-anyconnect-dll-hijac-JrcTOQMC>

二、接报漏洞情况

本周 CNNVD 接报漏洞 1493 个，其中信息技术产品漏洞（通用型漏洞）13 个，网络信息系统漏洞（事件型漏洞）1480 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 | 980 |
| 2 | 网神信息技术（北京）股份有限公司 | 429 |
| 3 | 北京天地和兴科技有限公司 | 30 |
| 4 | 山东华鲁科技发展股份有限公司 | 16 |
| 5 | 北京数字观星科技有限公司 | 13 |
| 6 | 任子行网络技术股份有限公司 | 8 |
| 7 | 北京圣博润高新技术股份有限公司 | 5 |
| 8 | 河南听潮盛世信息技术有限公司 | 5 |
| 9 | 北京威努特技术有限公司 | 3 |
| 10 | 山东云天安全技术有限公司 | 3 |
| 11 | 恒安嘉新（北京）科技股份公司 | 1 |
| 报送总计 | | 1493 |

三、接报漏洞预警情况

本周 CNNVD 接报漏洞预警 6 份。

| 序号 | 报送单位 | 预警总量 |
|----|---------------|------|
| 1 | 北京华云安信息技术有限公司 | 2 |

| | | |
|------|-----------------|---|
| 2 | 北京天融信网络安全技术有限公司 | 1 |
| 3 | 北京安天网络安全技术有限公司 | 1 |
| 4 | 北京华顺信安科技有限公司 | 1 |
| 5 | 内蒙古奥创科技有限公司 | 1 |
| 报送总计 | | 6 |