

信息安全漏洞周报

(2020 年第 7 期 总第 511 期)

信息安全测评中心

2020 年 2 月 23 日

根据国家信息安全漏洞库 (CNNVD) 统计, 本周 (2020 年 2 月 17 日至 2020 年 2 月 23 日) 安全漏洞情况如下:

公开漏洞情况

本周 CNNVD 采集安全漏洞 241 个, 与上周 (486 个) 相比减少了 48.72%。

接报漏洞情况

本周 CNNVD 接报漏洞 1209 个, 其中信息技术产品漏洞 (通用型漏洞) 81 个, 网络信息系统漏洞 (事件型漏洞) 1128 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 241 个，漏洞新增数量有所上升。从厂商分布来看 IBM 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 11.62%。新增漏洞中，超危漏洞 33 个，高危漏洞 48 个，中危漏洞 151 个，低危漏洞 9 个。相应修复率分别为 57.58%、81.25%、58.28% 和 44.44%。根据补丁信息统计，合计 150 个漏洞已有修复补丁发布，整体修复率为 62.24%。

（一）安全漏洞增长数量情况

本周 CNNVD 采集安全漏洞 241 个，与上周（468 个）相比减少了 48.72%。图 1 为近五周漏洞新增数量统计图。

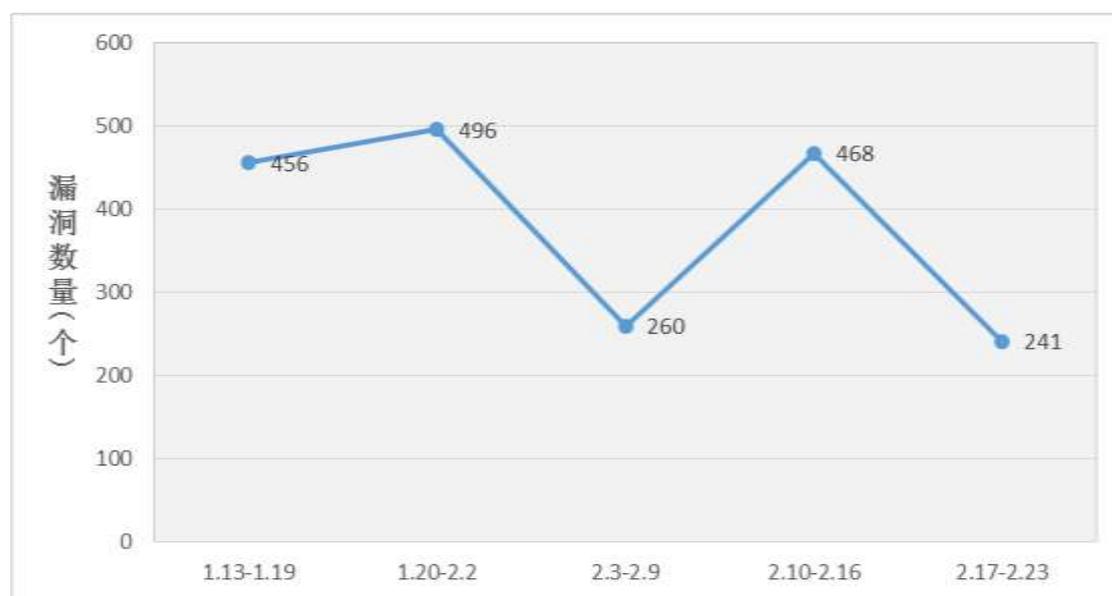


图 1 近五周漏洞新增数量统计图

（二）安全漏洞分布情况

从厂商分布来看，IBM 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	IBM	19	7.88%
2	Cisco	17	7.05%
3	Huawei	12	4.98%
4	Netsweeper	9	3.73%
5	Ansible	8	3.32%

本周国内厂商漏洞 15 个，华为公司漏洞数量最多，有 12 个。国内厂商漏洞整体修复率为 86.67%。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 11.62%。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	28	11.62%
2	缓冲区错误	16	6.64%
3	代码问题	13	5.39%
4	跨站请求伪造	11	4.56%
5	输入验证错误	10	4.15%
6	操作系统命令注入	9	3.73%
7	SQL 注入	9	3.73%
8	路径遍历	8	3.32%
9	信息泄露	6	2.49%
10	命令注入	5	2.07%
11	访问控制错误	4	1.66%
12	资源管理错误	4	1.66%
13	注入	3	1.24%
14	信任管理问题	2	0.83%
15	数据伪造问题	2	0.83%
16	加密问题	1	0.41%
17	权限许可和访问控制问题	1	0.41%

18	授权问题	1	0.41%
19	竞争条件问题	1	0.41%

(三) 安全漏洞危害等级与修复情况

本周共发布超危漏洞 33 个，高危漏洞 48 个，中危漏洞 151 个，低危漏洞 9 个。相应修复率分别为 57.58%、81.25%、58.28%和 44.44%。根据补丁信息统计，合计 150 个漏洞已有修复补丁发布，整体修复率为 62.24%。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	33	19	57.58%
2	高危	48	39	81.25%
3	中危	151	88	58.28%
4	低危	9	4	44.44%
合计		241	150	62.24%

(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-202002-1003	NEC	NEC Aterm WF1200C、Aterm WG1200CR 和 Aterm WG2600HS 操作系统命令注入漏洞	是	高危
2	信任管理问题	CNNVD-202002-985	Cisco	Cisco Smart Software Manager On-Prem 信任管理问题漏洞	是	超危
3	其他	CNNVD-202002-905	IBM	IBM Maximo Asset Management 安全漏洞	是	超危

1. NEC Aterm WF1200C、Aterm WG1200CR 和 Aterm WG2600HS 操作

系统命令注入漏洞（CNNVD-202002-1003）

NEC Aterm WF1200C 等都是日本电气（NEC）公司的一款无线路由器。

NEC Aterm WF1200C 1.2.1 及之前版本、Aterm WG1200CR 1.2.1 及之前版本和 Aterm WG2600HS 1.3.2 及之前版本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、命令等。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，补丁获取链接：

<https://jpn.nec.com/security-info/secinfo/nv20-005.html>

2. Cisco Smart Software Manager On-Prem 信任管理问题漏洞（CNNVD-202002-985）

Cisco Smart Software Manager On-Prem 是美国 Cisco 公司的一款用于 Cisco 产品许可证管理的组件。

Cisco Smart Software Manager On-Prem 7-202001 之前版本中的 High Availability (HA) 服务存在信任管理问题漏洞，该漏洞源于系统管理员无法控制带有默认静态密码的系统账户。远程攻击者可通过使用该账户利用该漏洞访问系统的敏感部分。

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-on-prem-static-cred-sL8rDs8>

3. IBM Maximo Asset Management 安全漏洞（CNNVD-202002-905）

IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。该方案能够在在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。

IBM Maximo Asset Management 7.5 版本、7.1 版本和 6.2 版本中存在提权漏洞。攻击者可利用该漏洞获取未授权的访问权限。

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/235239>

二、接报漏洞情况

本周 CNNVD 接报漏洞 1209 个，其中信息技术产品漏洞（通用型漏洞）81 个，网络信息系统漏洞（事件型漏洞）1128 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	491
2	网神信息技术（北京）股份有限公司	347
3	内蒙古洞明科技有限公司	100
4	广州锦行网络科技有限公司	67
5	太极计算机股份有限公司	37
6	北京华云安信息技术有限公司	30
7	上海谋乐网络科技有限公司	20
8	西安四叶草信息技术有限公司	20
9	浙江大华技术股份有限公司	16
10	北京启明星辰信息安全技术有限公司 ADLab	11

11	北京梆梆安全科技有限公司	11
12	北京圣溥润高新技术股份有限公司	10
13	北京数字观星科技有限公司	10
14	上海银基信息安全技术有限公司	7
15	北京邮电大学	6
16	北京圣博润高新技术股份有限公司	5
17	梆梆安全	5
18	湖南省金盾信息安全等级保护评估中心有限公司	4
19	河南听潮盛世信息技术有限公司	3
20	上海银基信息安全技术股份有限公司	3
21	北京山石网科信息技术有限公司	3
22	北京智游网安科技有限公司	2
23	北京天融信网络安全技术有限公司	1
报送总计		1209