国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 1 月 15 日-2018 年 1 月 28 日 **2018 年第 3 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**中**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 410 个，其中高危漏洞 128 个、中危漏洞 236 个、低危漏洞 46 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 139 个（占 34%），其中互联网上出现“Cobbler 命令注入漏洞、WordPress Gravity Upload Ajax 插件任意文件上传漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 532 个，与上周（498 个）环比增长 6%。

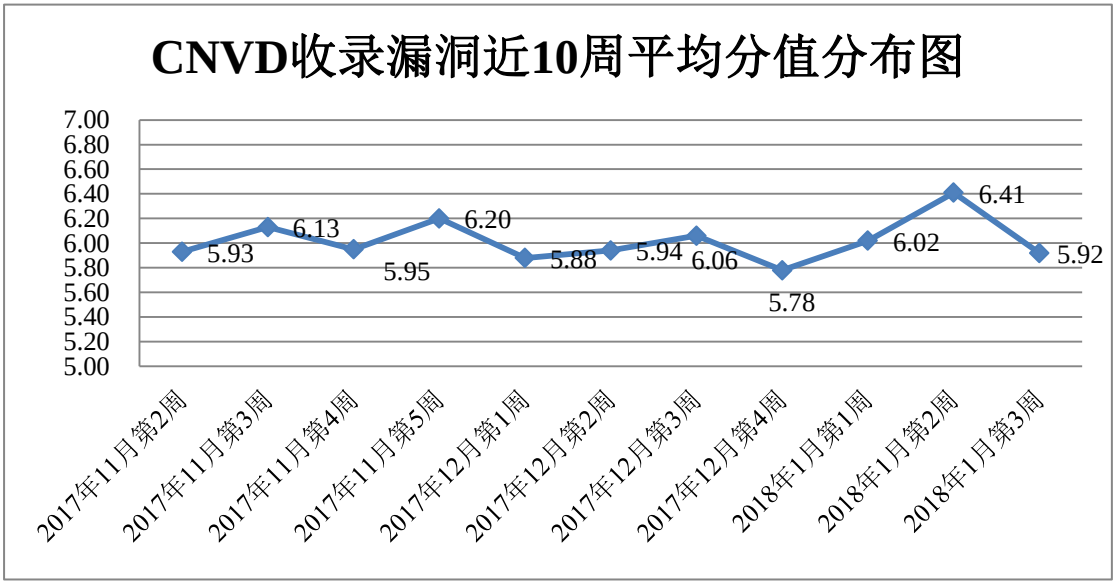

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，恒安嘉新、华为技术有限公司、东软、天融信、H3C 等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、安创科技、中新网络信息安全股份有限公司、漏斗社区、北京智游网安科技有限公司、邹平九零冰讯

网络科技有限公司、山石网科通信技术有限公司、中国电信股份有限公司网络安全产品运营中心及其他个人白帽子向 CNVD 提交了 532 个以事件型漏洞为主的原创漏洞。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
网神	233	233
恒安嘉新	223	0
华为技术有限公司	212	0
东软	205	1
天融信	156	6
H3C	145	0
启明星辰	132	0
中国电信集团系统集成有限责任公司	69	0
绿盟科技	65	0
杭州安恒信息技术有限公司	51	0
北京无声信息技术有限公司	45	0
卫士通信息产业股份有限公司	30	0
北京数字观星科技有限公司	25	0
漏洞盒子	18	18
西安四叶草信息技术有限公司	10	10
知道创宇	3	0
深圳市深信服电子科技有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
四川虹微技术有限公司（子午攻防实验室）	65	65
南京联成科技发展股份有限公司	11	11

安创科技	3	3
中新网络信息安全股份有限公司	3	3
漏斗社区	2	2
北京智游网安科技有限公司	2	2
邹平九零冰讯网络科技有限公司	1	1
山石网科通信技术有限公司	1	1
中国电信股份有限公司网络安全产品运营中心	1	1
CNCERT 山西分中心	18	18
CNCERT 新疆分中心	5	5
CNCERT 福建分中心	2	2
CNCERT 贵州分中心	1	1
CNCERT 湖南分中心	4	4
CNCERT 吉林分中心	2	2
CNCERT 广东分中心	1	1
个人	140	140
报送总计	1886	532

本周漏洞按类型和厂商统计

本周，CNVD 收录了 410 个漏洞。其中应用程序漏洞 197 个，web 应用漏洞 106 个，操作系统漏洞 39 个，安全产品漏洞 38 个，网络设备漏洞 30 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	197
web 应用漏洞	106
操作系统漏洞	39
安全产品漏洞	38
网络设备漏洞	30

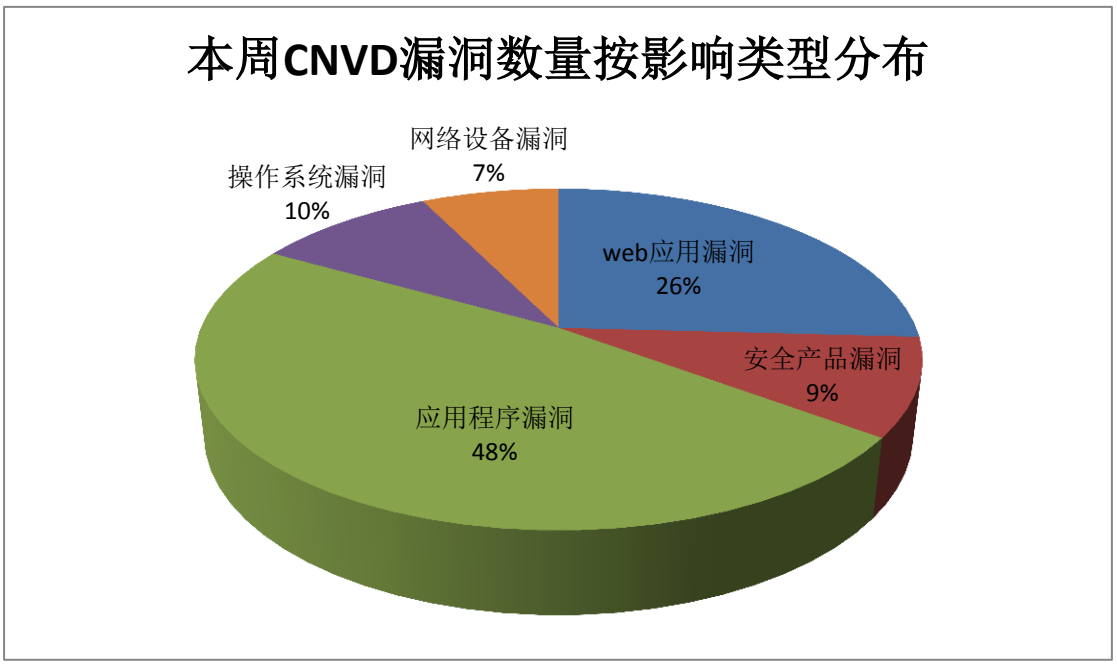

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Google、IBM 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	WordPress	56	14%
2	Google	34	8%
3	IBM	23	6%
4	Microsoft	22	5%
5	K7 Computing Pvt Ltd	17	4%
6	F5	14	3%
7	NetGain	13	3%
8	Trend Micro	10	2%
9	Cambium Networks	10	2%
10	其他	211	53%

本周行业漏洞收录情况

本周，CNVD 收录了 18 个电信行业漏洞，45 个移动互联网行业漏洞，21 个工控行业漏洞（如下图所示）。其中，“MikroTik RouterOS 远程代码执行漏洞、D-Link DIR 615/645/815 service.cgi 远程命令执行漏洞、PHOENIX CONTACT FL SWITCH 未授权

访问漏洞、Google Android Kernel Bluez 权限提升漏洞、Moxa MXview 权限提升漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

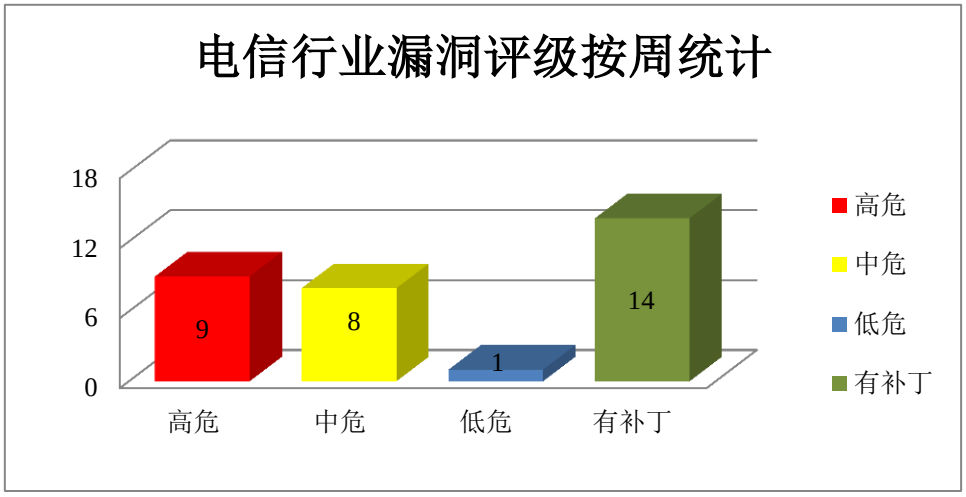

图 3 电信行业漏洞统计

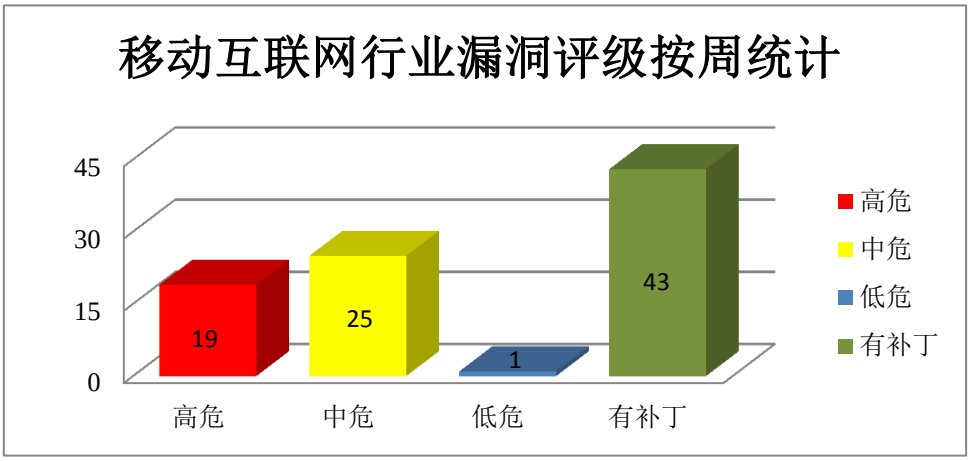

图 4 移动互联网行业漏洞统计

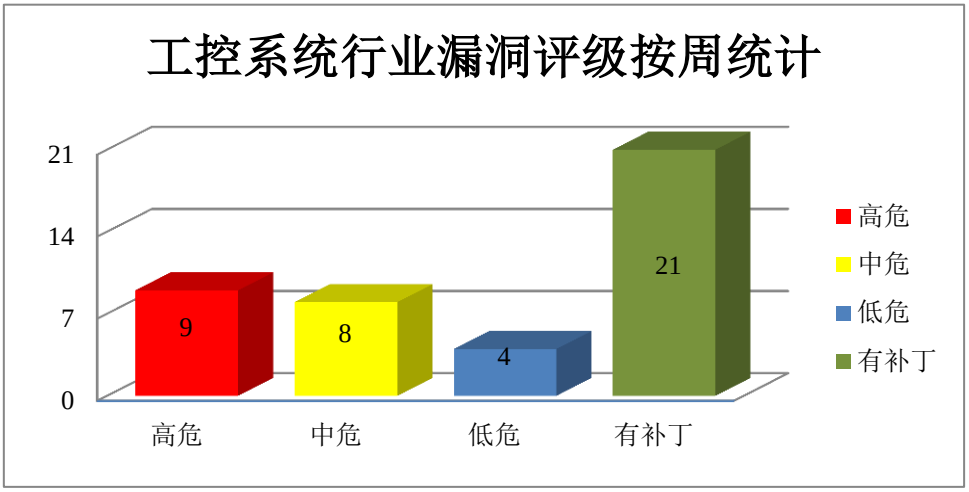

图 5 工控行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Intel AMT 存在高危漏洞

Intel AMT 是一种集成在芯片组中的嵌入式系统，独立于特定操作系统。本周，该产品被披露存在高危安全漏洞，攻击者可利用漏洞完全控制目标用户的笔记本电脑。

CNVD 收录的相关漏洞包括：Intel AMT 存在高危安全漏洞。上述漏洞的综合评级为“高危”。目前，厂商尚未发布漏洞修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-00925

2、Microsoft 产品安全漏洞

Microsoft Office 是美国微软（Microsoft）公司开发的一款办公软件套件产品。本周，上述产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Office 内存破坏漏洞（CNVD-2018-00884、CNVD-2018-00903、CNVD-2018-00904）、Microsoft Office 远程代码执行漏洞（CNVD-2018-00886、CNVD-2018-00887、CNVD-2018-00888、CNVD-2018-00889、CNVD-2018-00905）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-00884

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00903

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00904

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00886

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00887

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00888

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00889

http://www.cnvd.org.cn/flaw/show/CNVD-2018-00905

3、Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Closed-source 组件存在未明漏洞、Google Android Kernel Bluez 权限提升漏洞、Google Android Kernel WiFi 驱动程序权限提升漏洞、Google Android MediaTek MTK 权限提升漏洞、Google Android Qualcomm Bootloader 权限提升漏洞、Google Android Qualcommr Driver 权限提升漏洞、Google Android Qualcommr SOC 驱动程序权限提升漏洞、Google Android System(systemui)权限提升漏洞。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-01107

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01180

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01181

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01183

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01103

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01106

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01105

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01173

4、NetGain 产品安全漏洞

NetGain Enterprise Manager 是个端到端 IT 基础架构的监控平台。本周，上述产品被披露存在目录遍历漏洞，攻击者可利用漏洞访问或读取任意文件。

CNVD 收录的相关漏洞包括：NetGain Systems Enterprise Manager 目录遍历漏洞（CNVD-2018-01227、CNVD-2018-01228、CNVD-2018-01229、CNVD-2018-01230、CNVD-2018-01234、CNVD-2018-01235、CNVD-2018-01236、CNVD-2018-01237）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-01227

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01228

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01229

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01230

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01234

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01235

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01236

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01237

5、 D-Link DIR-629 和 DIR-823 远程栈溢出漏洞

D-Link DIR-629 和 DIR-823 都是友讯（D-Link）公司的无线路由器产品。本周，D-Link 被披露存在远程栈溢出漏漏洞，攻击者可利用漏洞导致缓冲区溢出。目前，厂商尚未发布漏洞修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。参考链接：http://www.cnvd.org.cn/flaw/show/CNVD -2018-00924

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。参考链接：http://www.cnvd.org.cn/flaw/list.htm

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2018-01084	D-Link DIR 615/645/815 service.cgi 远程命令执行漏洞	高	用户可联系供应商获得补丁信息：http://us.dlink.com/
CNVD-2018-01088	Desdev DedeCMS SQL 注入漏洞（CNVD-2018-01088）	高	厂商已发布漏洞修复程序，请及时关注更新：http://www.dedecms.com/
CNVD-2018-01146	多款 F5 产品竞争条件漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K24465120
CNVD-2018-01147	多款 F5 产品拒绝服务漏洞（CNVD-2018-01147）	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K07369970
CNVD-2018-01162	IKARUS anti.virus 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://www.greyhathacker.net/?p=995
CNVD-2018-01164	多款 F5 产品拒绝服务漏洞（CNVD-2018-01164）	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K43322910
CNVD-2018-01166	多款 F5 产品拒绝服务漏洞（CNVD-2018-01166）	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K25033460
CNVD-2018-01282	WordPress Dbox 3D Slider Lite 插件 SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://slidervilla.com/dbox-lite/
CNVD-2018-01320	Netgain Enterprise Manager 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

			http://www.netgain-systems.com.cn/
CNVD-2018-01321	NetGain Enterprise Manager 命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.netgain-systems.com.cn/

小结：本周，Intel 被披露存在高危安全漏洞，攻击者可利用漏洞完全控制目标用户的笔记本电脑。此外，Microsoft、Google、NetGain 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或访问或读取任意文件等。另外，D-Link 被披露存在远程栈溢出漏漏洞，攻击者可利用漏洞导致缓冲区溢出。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周漏洞要闻速递

1. ISC BIND9 爆出 DoS 漏洞 BIND 9.0 后所有版本受影响

近日，ISC BIND 爆出高危 DoS 漏洞 ，CVE 编号 CVE-2017-3145， 该错误存在于 守护进程 库 netaddr.c 模块 中。禁用 DNSSEC 验证是一种解决方法，但是 ISC 公告称建议自从 BIND 9.0.0（2000 年发布）以来的所有版本都需要进行修补。BIND 在上游递归获取上下文中，对清除操作进行了不正确的排序，在某些情况下导致了 use-after-free 错误，进而触发断言失败及命名崩溃。

参考链接：http://toutiao.secjia.com/cve-2017-3145

2. MySQL 多个远程安全漏洞大批版本受影响

近日，MySQL 爆出多个远程安全漏洞，CVE 编号 CVE-2018-2562 及 CVE-2018-2591，CVE-2018-2562 漏洞影响版本包括，5.5.58 及之前版本，5.6.38 及之前版本，5.7.19 之前版本。CVE-2018-2591 漏洞影响版本包括 5.6.38 及之前版本，5.7.19 及之前版本。在服务器分区中，MySQL 服务器很容易出现远程安全漏洞。该漏洞可以在“MySQL”协议上被利用。

参考链接：http://toutiao.secjia.com/cve-2018-2562-91

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中

心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82991537