国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 10 月 29 日-2018 年 11 月 04 日 **2018 年第 44 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 203 个，其中高危漏洞 90 个、中危漏洞 106 个、低危漏洞 7 个。漏洞平均分值为 6.39。本周收录的漏洞中，涉及 0day 漏洞 37 个（占 18%），其中互联网上出现“Wecodex Restaurant CMS 'Login' SQL 注入漏洞、多款 Tenda 产品 httpd 缓冲区溢出漏洞”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 1005 个，与上周（914 个）环比增长 10%。

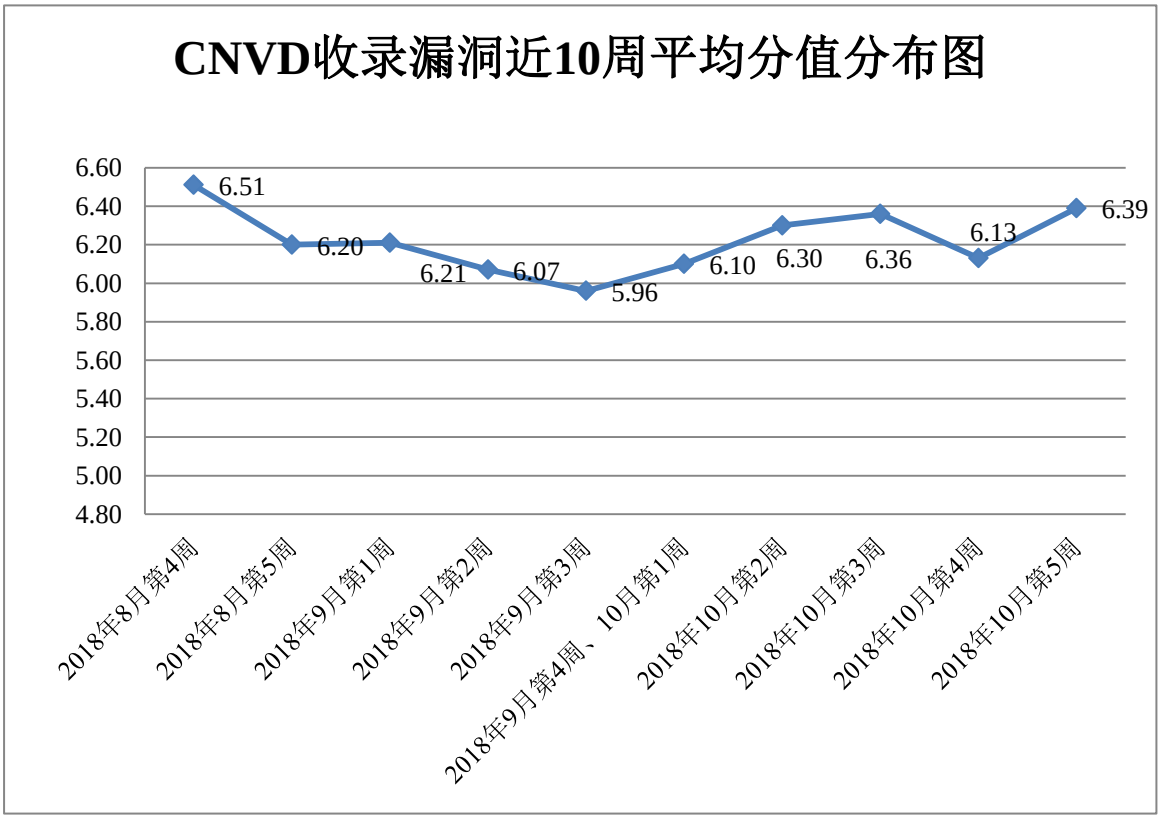

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 1 起，向保险、能源等重要行业单位通报漏洞事件 11 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 130 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 17 起，向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 9 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

郑州路之易科技有限公司、灵宝简好网络科技有限公司、长春凌展软件有限责任公司、中国科技创新网、武汉噢易云计算股份有限公司、北京新启科技有限公司、大米 CMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技股份有限公司、新华三技术有限公司、华为技术有限公司、北京数字观星科技有限公司、中国电信集团系统集成有限责任公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、北京圣博润高新技术股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、任子行网络技术股份有限公司、中新网络信息安全股份有限公司、内蒙古奥创科技有限公司、山石网科通信技术有限公司、安徽锋刃信息科技有限公司、北京明朝万达科技股份有限公司（安元实验室）、北京市电子产品质量检测中心、江苏省信息安全测评中心及其他个人白帽子向 CNVD 提交了 1005 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 694 条原创漏洞信息。

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
360 网神（补天平台）	518	518
哈尔滨安天科技股份有限公司	186	0
新华三技术有限公司	181	0
华为技术有限公司	179	0
漏洞盒子	176	176
北京数字观星科技有限公司	135	0

中国电信集团系统集成有限责任公司	83	0
北京神州绿盟科技有限公司	71	0
深信服科技股份有限公司	28	0
北京天融信网络安全技术有限公司	25	9
恒安嘉新(北京)科技股份公司	20	0
北京知道创宇信息技术有限公司	4	2
杭州安恒信息技术有限公司	3	3
山东云天安全技术有限公司	84	84
北京圣博润高新技术股份有限公司	32	32
远江盛邦（北京）网络安全科技股份有限公司	23	23
任子行网络技术股份有限公司	8	8
中新网络信息安全股份有限公司	8	8
内蒙古奥创科技有限公司	5	5
山石网科通信技术有限公司	3	3
安徽锋刃信息科技有限公司	3	3
北京明朝万达科技股份有限公司（安元实验室）	1	1
北京市电子产品质量检测中心	1	1
江苏省信息安全测评中心	1	1
CNCERT 山西分中心	32	32
CNCERT 甘肃分中心	6	6
CNCERT 上海分中心	6	6
CNCERT 四川分中心	6	6

CNCERT 新疆分中心	5	5
CNCERT 贵州分中心	3	3
CNCERT 湖南分中心	3	3
CNCERT 北京分中心	2	2
CNCERT 内蒙古分中心	2	2
CNCERT 海南分中心	1	1
个人	62	62
报送总计	1906	1005

本周漏洞按类型和厂商统计

本周，CNVD 收录了 200 个漏洞。应用程序漏洞 93 个，WEB 应用漏洞 72 个，网络设备漏洞 16 个，操作系统漏洞 15 个，安全产品漏洞 7 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	93
WEB 应用漏洞	72
网络设备漏洞	16
操作系统漏洞	15
安全产品漏洞	7

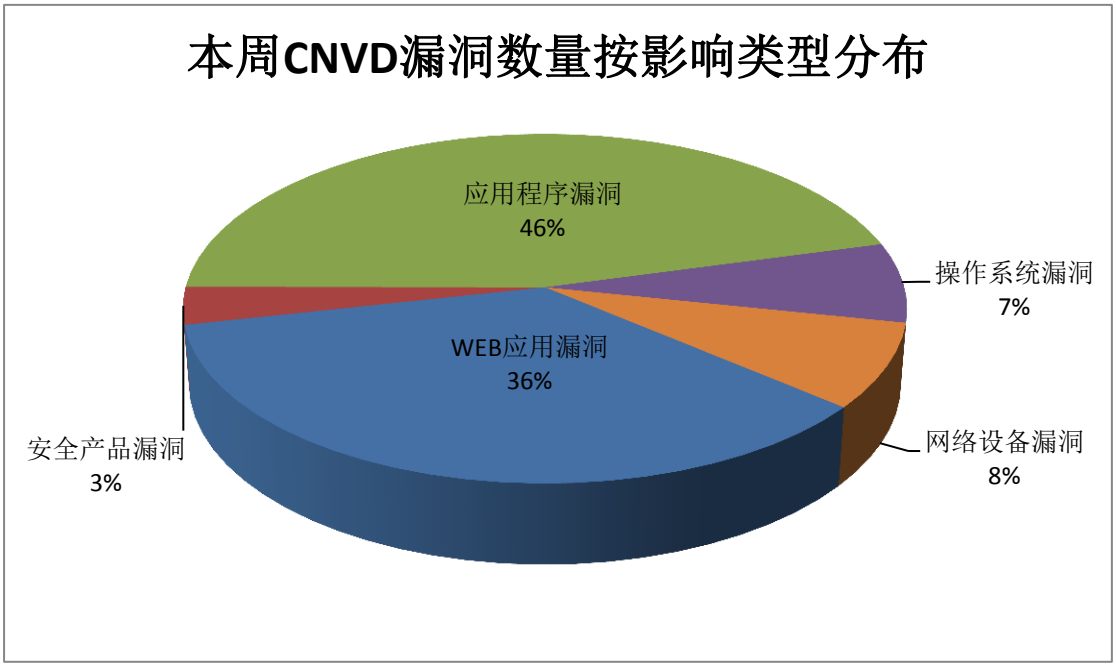

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Apple、Google 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	IBM	16	8%
2	Apple	14	7%
3	Google	14	7%
4	GNU	11	5%
5	Foxit	8	4%
6	上海亿速网络科技有限公司	8	4%
7	镇江市云优网络科技有限公司	6	3%
8	Envato Pty Ltd.	5	2%
9	Apache	4	2%
10	其他	117	58%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，8 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-823G 存在命令注入漏洞、IBM WebSphere

Commerce 开放重定向漏洞、Apple iOS FaceTime 内存破坏漏洞、Foxit Reader 和 Foxit PhantomPDF for Windows 内存错误引用漏洞（CNVD-2018-22404）、GAIN Electronic Co. Ltd SAGA1-L Series 命令伪造漏洞”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/

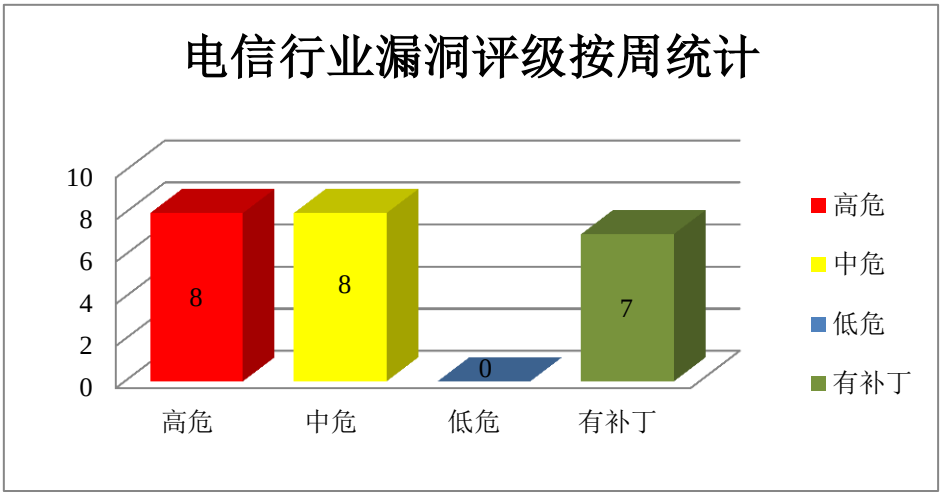

图 3 电信行业漏洞统计

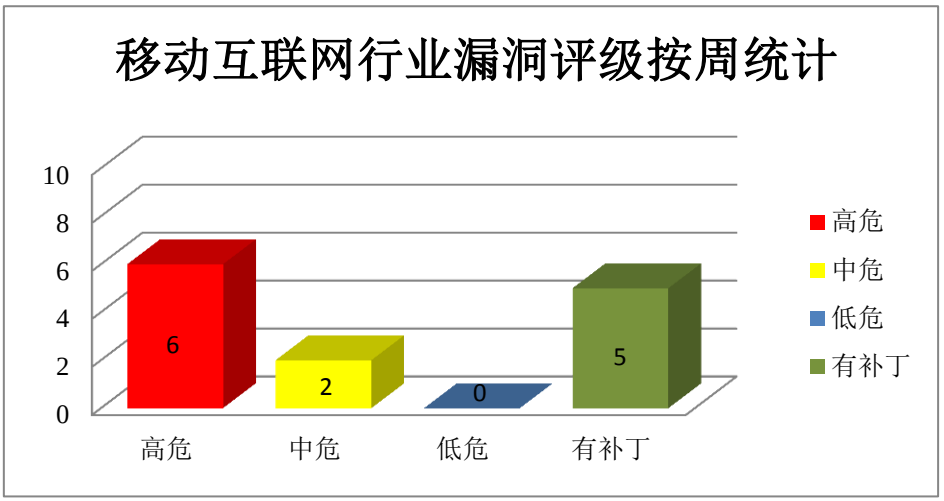

图 4 移动互联网行业漏洞统计

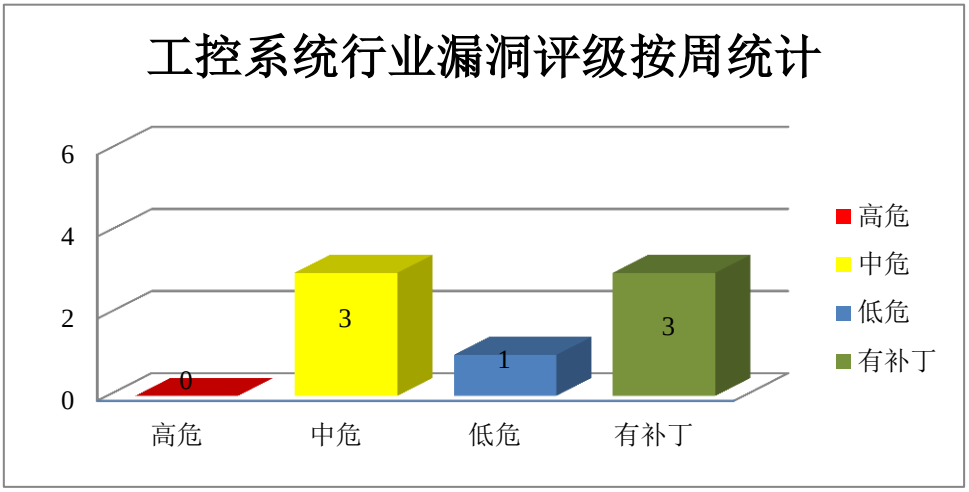

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM WebSphere Application Server（WAS）是一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。IBM WebSphere Commerce 是一套电子商务解决方案。IBM Daeja ViewONE Virtual 是一款文档查看器，支持查看 TIFF、PDF 和基于 Office 的文档。IBM Kenexa LCMS Premier on Cloud 是一套可调节的用于开发、维护和提供高效的员工培训的学习内容管理系统 (LCMS)。IBM Security Access Manager 是一款应用于信息安全管理的产品。IBM FlashSystem 840 MTMs 9840-AE1 等都是企业级存储解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行未授权的操作，执行任意代码，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM WebSphere Commerce 信息泄露漏洞（CNVD-2018-22087、CNVD-2018-22088）、IBM WebSphere Commerce 开放重定向漏洞、IBM Daeja ViewONE Virtual XXE 漏洞、IBM WebSphere Application Server Liberty OpenID Connect 代码执行漏洞、IBM Kenexa LCMS Premier on Cloud SQL 注入漏洞、IBM Security Access Manager 未授权操作漏洞、多款 IBM 产品 GUI 权限提升漏洞。其中，除“IBM WebSphere Commerce 信息泄露漏洞（CNVD-2018-22087、CNVD-2018-22088）”外，其余漏洞的综合评级为“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-2018-22087

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22088

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22089

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22367

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22368

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22371

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22370

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22375

2、Apple 产品安全漏洞

Apple macOS Sierra 是为 Mac 计算机所开发的一套专用操作系统。Apple iOS 是为移动设备所开发的一套操作系统。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞以系统权限执行任意代码（内存破坏）。

CNVD 收录的相关漏洞包括：Apple macOS mDNSOffloadUserClient 内存破坏漏洞、Apple iOS FaceTime 内存破坏漏洞、Apple macOS Sierra Kernel 内存破坏漏洞（CNVD-2018-22359、CNVD-2018-22360、CNVD-2018-22361、CNVD-2018-22363、CNVD-2018-22366）、Apple macOS 内存损坏漏洞（CNVD-2018-22365）。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-2018-22356

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22358

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22359

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22360

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22361

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22363

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22366

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22365

3、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，造成堆破坏。

CNVD 收录的相关漏洞包括：Google Chrome Blink 内存错误引用漏洞（CNVD-2018-22389）、Google Chrome Blink 信息泄露漏洞、Google Chrome 安全绕过漏洞（CNVD-2018-22395、CNVD-2018-22396）、Google Chrome Skia 堆缓冲区溢出漏洞（CNVD-2018-22399）、Google Chrome PDFium 内存错误引用漏洞（CNVD-2018-22400、CNVD-2018-22401）、Google Chrome V8 类型混淆漏洞（CNVD-2018-22402）。其中，除“Google Chrome Blink 信息泄露漏洞、Google Chrome 安全绕过漏洞（CNVD-2018-22395、CNVD-2018-22396）”外，其余漏洞的综合评级为“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-2018-22389

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22393

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22395

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22396

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22399

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22400

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22401

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22402

4、Foxit 产品安全漏洞

CFoxit Reader for Windows 是一款基于 Windows 平台的 PDF 文档阅读器。Foxit PhantomPDF for Windows 是它的商业版。本周，该产品被披露存在内存错误引用漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Foxit Reader for Windows 内存错误引用漏洞（CNVD-2018-22397）、Foxit Reader 和 Foxit PhantomPDF for Windows 内存错误引用漏洞（CNVD-2018-22404、CNVD-2018-22405、CNVD-2018-22406、CNVD-2018-22407、CNVD-2018-22408、CNVD-2018-22410、CNVD-2018-22409）。上述漏洞的综合评级为“高危”。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-2018-22397

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22404

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22405

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22406

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22407

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22408

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22410

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22409

5、GNU Binutils 'elf_link_input_bfd'函数拒绝服务漏洞

GNU Binutils（又名 GNU Binary Utilities 或 binutils）是 GNU 计划开发的一组编程语言工具程序，它主要用于处理多种格式的目标文件，并提供有连接器、汇编器和其他用于目标文件和档案的工具。Binary File Descriptor（BFD）library（又名 libbfd）是其中的一个以各种格式便携式操作对象文件的库。本周，GNU Binutils 被披露存在拒绝服务漏洞。远程攻击者可借助特制的 ELF 文件利用该漏洞造成拒绝服务（空指针逆向引用）。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-2018-22386

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-2018-21951	D-Link DIR-823G 存在命令注入漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：http://www.dlink.com.cn/
CNVD-2018-21952	D-Link DIR-823G 存在越权访问漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：http://www.dlink.com.cn/
CNVD-2018-22150	PHP Dashboards 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：https://codecanyon.net/item/php-dashboards-v50-brand-new-enterprise-edition/21540104
CNVD-2018-22151	PHP Dashboards 'email' 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://codecanyon.net/item/php-dashboards-v40-collaborative-social-dashboards/19314871
CNVD-2018-22152	MySQL Blob Uploader 'home-filet-edit.php' 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：https://codecanyon.net/item/mysql-file-and-image-uploader-and-sharing-blob-file-server/17748300
CNVD-2018-22154	Combine CMS 存在多个漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.combine-project.eu/
CNVD-2018-22244	Dell EMC Integrated Data Protection Appliance 未记录账户漏洞	高	用户可联系供应商获得补丁信息：https://download.emc.com/downloads/DL89669_Idpa_post_update_2.1.0.599285.tar.gz
CNVD-2018-22245	EE 4GEE HH70 Home Router 硬编码 Root SSH 凭证漏洞	高	用户可联系供应商获得补丁信息：https://shop.ee.co.uk/dongles/pay-monthly-mobile-broadband/4gee-router/details
CNVD-2018-22309	多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2018-22309）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/zh-cn/HT209196
CNVD-2018-22362	多款 Apple 产品 Kernel 内存初始化漏洞（CNVD-2018-22362）	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT209193

小结：本周，IBM 被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行未

授权的操作，执行任意代码，发起拒绝服务攻击。此外，Apple、Google、Foxit 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，造成堆破坏，以系统权限执行任意代码（内存破坏）。另外，GNU Binutils 被披露存在拒绝服务漏洞。远程攻击者可借助特制的 ELF 文件利用该漏洞造成拒绝服务（空指针逆向引用）。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、多款 Tenda 产品 httpd 缓冲区溢出漏洞

验证描述

Tenda AC7 等都是中国腾达（Tenda）公司的无线路由器产品。httpd 是其中的一个 HTTP 服务器组件。

多款 Tenda 产品中的 httpd 存在缓冲区溢出漏洞。攻击者可利用该漏洞造成拒绝服务（覆盖函数的返回地址）。

验证信息

POC 链接：https://github.com/zsjevilhex/iot/blob/master/route/tenda/tenda-08/Tenda.md

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-22314

信息提供者

恒安嘉新(北京)科技股份公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. 英特尔超线程 CPU 出现新漏洞

安全人员近期发现了一个新的因特尔超线程 CPU 漏洞，是一个非常严重的旁注漏洞。该漏洞可使攻击者从同一 CPU 内核中运行的其他进程中找出受保护的敏感数据（如密码和加密密钥），并启用 CPU 的多线程功能。该漏洞被命名为 PortSmash（CVE-2018-5407），现在已被列为与 Meltdown 和 Spectre 等漏洞同等级别。

参考链接：https://thehackernews.com/2018/11/portsmash-intel-vulnerability.html

2. BleedingBit 蓝牙芯片远程代码执行漏洞

安全研究人员最近公布了两个蓝牙芯片漏洞的漏洞细节，并将之命名为 BleedingBit。这两个漏洞可以让攻击者实现远程代码执行，因为涉及到非常多的物联网设备，包括一些医学设备如胰岛素泵、心脏起搏器等，所以这两个漏洞的危害极其严重。

参考链接：https://www.anquanke.com/post/id/163307

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