国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 02 月 25 日-2019 年 03 月 03 日 **2019 年第 9 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 379 个，其中高危漏洞 152 个、中危漏洞 190 个、低危漏洞 37 个。漏洞平均分值为 5.98。本周收录的漏洞中，涉及 0day 漏洞 227 个（占 60%），其中互联网上出现“WordPress 插件 Advanced Custom Fields Pro SQL 注入漏洞、Nokia 8810 4G 设备 KaiOS Gecko 组件拒绝服务漏洞”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 1944 个，与上周（2374 个）环比下降 18%。

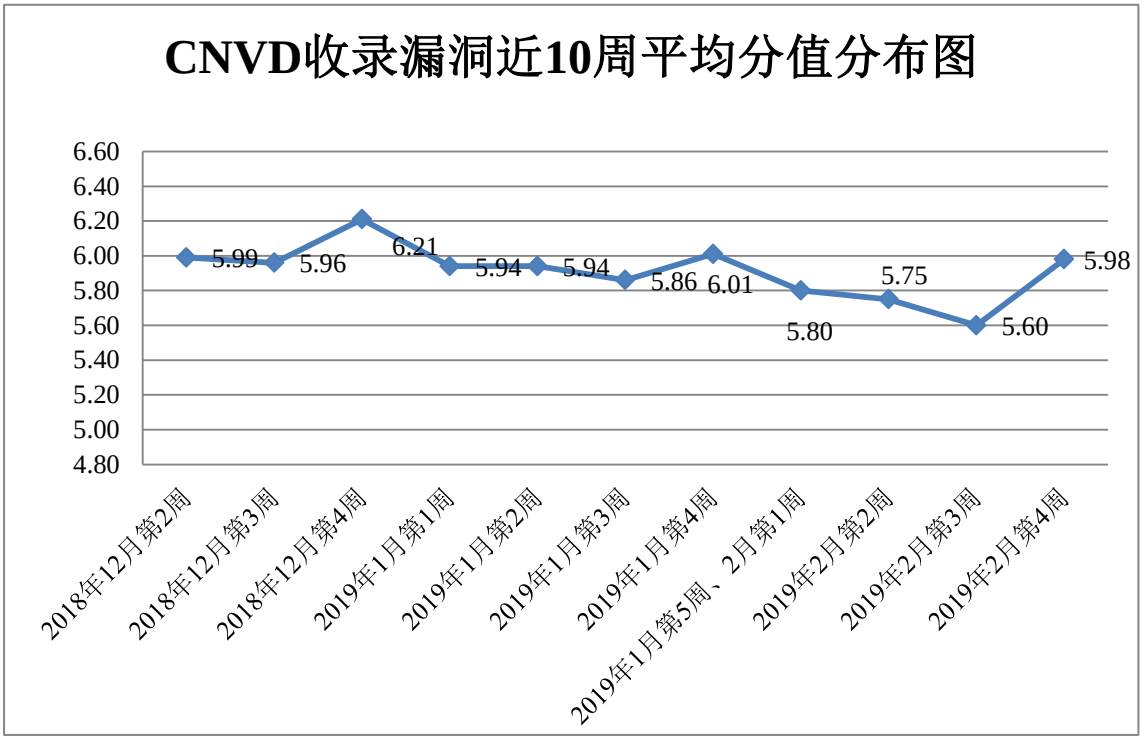

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向银行、保险、能源等重要行业

单位通报漏洞事件 14 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 526 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 108 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 21 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：

同望科技股份有限公司、北京小米科技有限责任公司、济南爱程网络科技有限公司、常州市青之峰网络科技有限公司、北京金和网络股份有限公司、上海证大喜马拉雅网络科技有限公司、河南汉申网络科技有限公司、上海鹏达计算机系统开发有限公司、深圳市沃仕达科技有限公司、南充市老虎云网络技术有限公司、上海卓卓网络科技有限公司、重庆然宇网络科技有限公司、南京马普科技有限公司、深圳市信锐网科技术有限公司、镇江市云优网络科技有限公司、深圳市易智达信息技术有限公司、武汉达梦数据库有限公司、北京五指互联科技有限公司、广州南方卫星导航仪器有限公司、成都天睿信息技术有限公司、帝国软件、米酷资源网、国防工业出版社、WMCMS 团队、SeaCMS、SchoolCMS、TechCandy 和 WebCzech。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、华为技术有限公司、北京数字观星科技有限公司、四川无声信息技术有限公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、中新网络信息安全股份有限公司、安徽锋刃信息科技有限公司、山东华鲁科技发展股份有限公司、北京圣博润高新技术股份有限公司、山东云天安全技术有限公司、河南信安世纪科技有限公司、山石网科通信技术股份有限公司、成都安美勤信息技术股份有限公司、江苏保旺达软件技术有限公司、江西安服信息产业有限公司、三门峡崤云安全服务有限公司、山东九州信泰信息科技股份有限公司、重庆市信息通信咨询设计院有限公司及其他个人白帽子向 CNVD 提交了 1944 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1419 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
斗象科技（漏洞盒子）	909	909
360 网神（补天平台）	510	510
哈尔滨安天科技集团股份有限公司	167	0
北京天融信网络安全技术有限公司	144	17

华为技术有限公司	111	0
北京数字观星科技有限公司	102	0
四川无声信息技术有限公司	78	78
北京启明星辰信息安全技术有限公司	49	2
中国电信集团系统集成有限责任公司	40	0
厦门服云信息科技有限公司	48	0
新华三技术有限公司	46	0
北京神州绿盟科技有限公司	41	0
深信服科技股份有限公司	37	0
恒安嘉新(北京)科技股份公司	27	0
北京知道创宇信息技术有限公司	2	0
国瑞数码零点实验室	47	47
中新网络信息安全股份有限公司	47	47
安徽锋刃信息科技有限公司	29	29
山东华鲁科技发展股份有限公司	20	20
北京圣博润高新技术股份有限公司	10	10
山东云天安全技术有限公司	10	10
河南信安世纪科技有限公司	8	8
山石网科通信技术股份有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
江苏保旺达软件技术有限公司	1	1
江西安服信息产业有限公司	1	1

三门峡崤云安全服务有限公司	1	1
山东九州信泰信息科技股份有限公司	1	1
重庆市信息通信咨询设计院有限公司	1	1
CNCERT 上海分中心	15	15
CNCERT 吉林分中心	12	12
CNCERT 贵州分中心	11	11
CNCERT 山西分中心	7	7
CNCERT 四川分中心	5	5
CNCERT 北京分中心	3	3
CNCERT 陕西分中心	3	3
CNCERT 浙江分中心	3	3
CNCERT 内蒙古分中心	2	2
CNCERT 天津分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 河南分中心	1	1
个人	185	185
报送总计	2739	1944

本周漏洞按类型和厂商统计

本周，CNVD 收录了 379 个漏洞。安全产品漏洞 2 个，应用程序漏洞 196 个，WEB 应用漏洞 137 个，网络设备漏洞 30 个，操作系统漏洞 13 个，安全产品漏洞 2 个，数据库漏洞 1 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	196
WEB 应用漏洞	137

网络设备漏洞	30
操作系统漏洞	13
安全产品漏洞	2
数据库漏洞	1

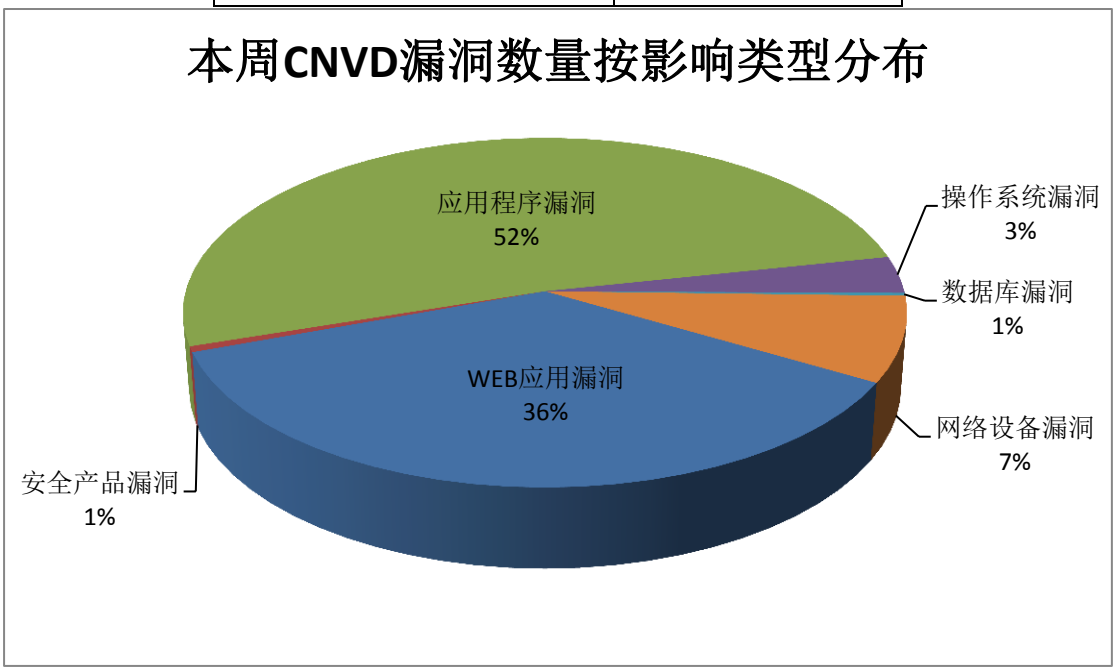

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Adobe、Intel 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	18	4%
2	Adobe	17	4%
3	Intel	15	4%
4	Drobo	14	4%
5	IBM	14	4%
6	Google	12	3%
7	Netwide Assembler(NASM)	10	3%
8	Rdesktop	10	3%
9	Mozilla	10	3%
10	其他	259	68%

本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞，26 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Cisco Webex Meetings Desktop App 和 Cisco Webex Productivity Tools 操作系统命令注入漏洞、Brocade Fabric OS 权限提升漏洞（CNVD-2019-05926）、Cisco RV110W、RV130W 和 RV215W 远程命令执行漏洞”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/

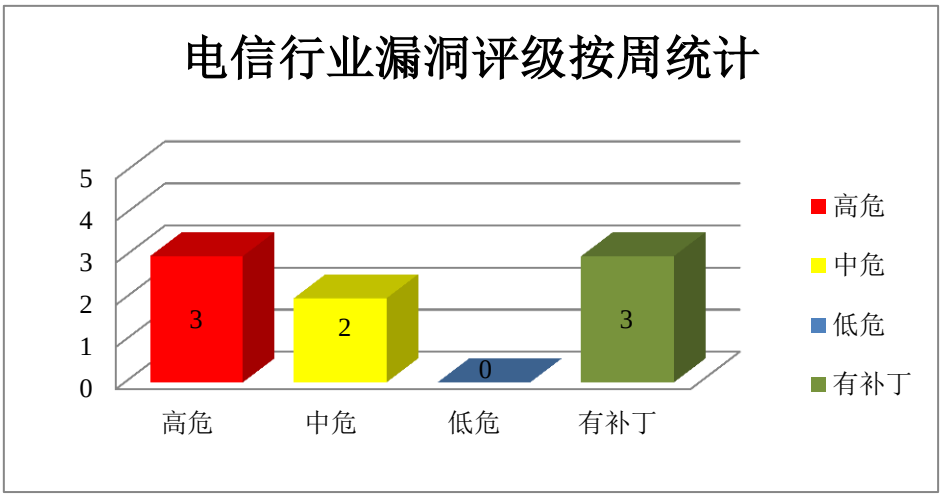

图 3 电信行业漏洞统计

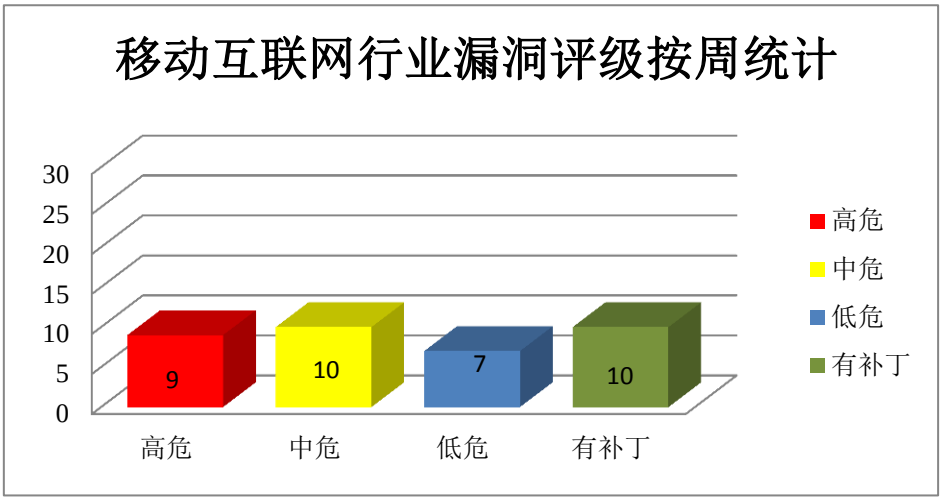

图 4 移动互联网行业漏洞统计

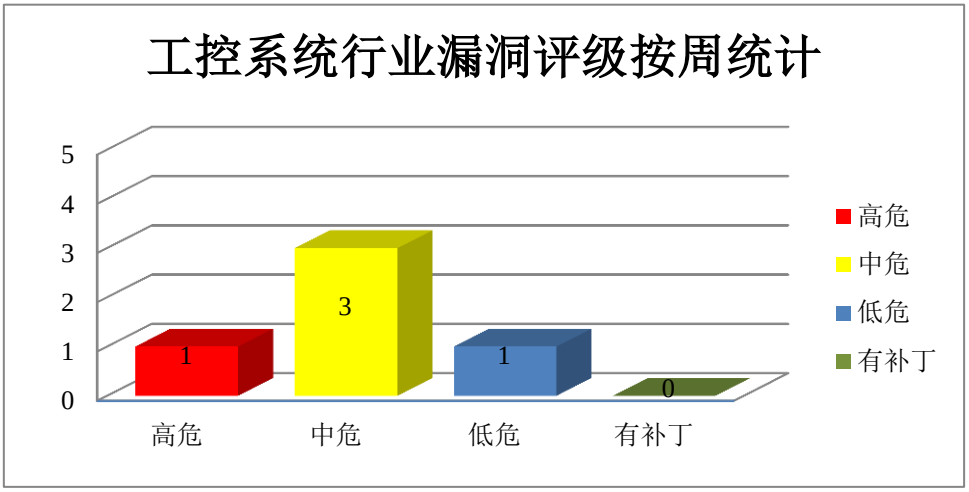

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 是一套 PDF 文件编辑和转换工具，Adobe Reader 是一套 PDF 文档阅读软件。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码（越界写入）。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2019-05308、CNVD-2019-05316、CNVD-2019-05317、CNVD-2019-05318、CNVD-2019-05319、CNVD-2019-05321、CNVD-2019-05320、CNVD-2019-05322）。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-2019-05308

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05316

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05317

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05318

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05319

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05321

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05320

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05322

2、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Firefox ESR 是 Firefox 的一个延长支持版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过沙盒，获取敏感信息，执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2019-05563）、Mozilla Firefox 权限提升漏洞（CNVD-2019-05566）、Mozilla Firefox 内存破坏漏洞（CNVD-2019-05564、CNVD-2019-05567、CNVD-2019-05568）、Mozilla Firefox 内存错误引用漏洞（CNVD-2019-05569）、Mozilla Firefox 信息泄露漏洞（CNVD-2019-05570）、Mozilla Firefox 和 Firefox ESR 整数溢出漏洞（CNVD-2019-05571）。其中，除“Mozilla Firefox 内存破坏漏洞（CNVD-2019-05568）、Mozilla Firefox 信息泄露漏洞（CNVD-2019-05570）”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-2019-05563
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05566
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05564
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05567
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05568
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05569
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05570
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05571

3、IBM 产品安全漏洞

IBM Security Identity Governance and Intelligence（IGI）是一套身份治理解决方案。IBM Security Identity Manager 是一套身份管理和治理解决方案。IBM Tivoli Storage Manager Operations Center 是一套下一代简化备份管理解决方案。本周，上述产品被披露存在信息泄露漏洞，攻击者可利用漏洞在 Web UI 中注入任意的 JavaScript 代码，获取敏感信息等。

CNVD 收录的相关漏洞包括：IBM Security Identity Governance and Intelligence 信息泄露漏洞（CNVD-2019-05281、CNVD-2019-05282、CNVD-2019-05515、CNVD-2019-05557）、IBM Security Identity Governance Virtual Appliance 跨站脚本漏洞、IBM Security Identity Manager 代码注入漏洞、IBM Tivoli Storage Manager Operations Center 跨站脚本漏洞（CNVD-2019-05656、CNVD-2019-05661）。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-2019-05281
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05282
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05515
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05516
http://www.cnvd.org.cn/flaw/show/CNVD-2019-05557

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05561

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05656

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05661

4、rdesktop 产品安全漏洞

rdesktop 是一个用于连接到 Windows 远程桌面服务的开源 UNIX 客户端。本周，该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，执行任意代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：rdesktop 堆缓冲区溢出漏洞、rdesktop process_plane()函数堆缓冲区溢出漏洞、rdesktop 整数溢出漏洞（CNVD-2019-05894、CNVD-2019-05895）、rdesktop process_secondary_order()函数越界读取漏洞、rdesktop rdpsnd_process_ping()函数越界读取漏洞、rdesktop 堆缓冲区溢出漏洞（CNVD-2019-05896）、rdesktop 越界读取漏洞。其中，除“rdesktop process_secondary_order()函数越界读取漏洞、rdesktop rdpsnd_process_ping()函数越界读取漏洞、rdesktop 越界读取漏洞”外，其余漏洞的综合评级为“高危”。目前，厂商尚未发布上述漏洞的修补程序。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-2019-05891

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05892

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05894

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05895

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05898

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05899

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05896

http://www.cnvd.org.cn/flaw/show/CNVD-2019-05897

5、Intel Data Center Manager SDK 文件权限提升漏洞

Intel Data Center Manager SDK 是一款数据中心管理器 SDK（软件开发工具包）。本周，Intel Data Center Manager SDK 被披露存在权限提升漏洞。攻击者利用该漏洞实现权限提升。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-2019-05272

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-2019-05262	Drupal 任意 PHP 代码执行漏洞（CNVD-2019-05262）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.drupal.org/sa-core-2019-00

			3
CNVD-2019-05264	Wibu-Systems WibuKey 权限提升漏洞	高	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.wibu.com/
CNVD-2019-05278	Intel Unite App 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00214.html
CNVD-2019-05289	Teracue ENC-400 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.teracue.com/
CNVD-2019-05297	ThinkPHP 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.thinkphp.cn/
CNVD-2019-05441	Ansible 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：https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10875
CNVD-2019-05879	Nablarch 拒绝服务漏洞	高	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://nablarch.github.io/
CNVD-2019-05901	Microsoft Outlook 远程代码执行漏洞（CNVD-2019-05901）	高	厂商已发布漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8587
CNVD-2019-05902	Cisco RV110W、RV130W 和 RV215W 远程命令执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex
CNVD-2019-05910	WordPress PHP 对象注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/

小结：本周，Adobe 被披露存在缓冲区溢出漏洞，攻击者可利用漏洞执行任意代码（越界写入）。此外，Mozilla、IBM、rdesktop 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过沙盒，获取敏感信息，执行任意代码，发起拒绝服务攻击等。另外，Intel Data Center Manager SDK 被披露存在权限提升漏洞。攻击者利用该漏洞实现权限提升。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、WordPress 插件 Advanced Custom Fields Pro SQL 注入漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

WordPress 插件 Advanced Custom Fields Pro SQL 注入漏洞。该漏洞是由于程序在 SQL 查询中使用用户提供的数据之前，未能充分过滤用户提供的数据。允许攻击者利用漏洞破坏应用程序、读取、访问或修改数据，或利用基础数据库中的潜在漏洞。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=32094

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-05445

信息提供者

CNVD 工作组

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. Thunderclap 攻击出现，影响 Thunderbolt 接口设备

研究人员发现 Thunderbolt 接口存在漏洞，暴露在 DMA（直接内存访问）攻击当中。可以本地访问 Thunderbolt 设备的潜在攻击者可以利用恶意的外接设备发起攻击。这一系列漏洞被命名为“Thunderclap”，可被攻击者利用，获取最高系统权限并运行任意代码，并窃取“密码、银行登录信息、加密密钥、隐私文件、浏览信息”等隐私信息。Windows、macOS、Linux 或 FreeBSD 等运行 Thunderbolt 的系统都可能受到影响。用户可以通过完全禁用 Thunderbolt 接口的方式来保护设备安全。

参考链接：https://www.bleepingcomputer.com/news/security/thunderclap-vulnerabilities-allow-attacks-using-thunderbolt-peripherals/

2. 软件故障导致 Lime 电动滑板车锁定

瑞士和新西兰的用户报告，他们的电动滑板车车轮在行驶过程中突然锁定，导致他们摔倒在地，有数十人因此受伤。在相关报道披露之后，Lime 于今年一月在瑞士停止了其电动滑板车租赁服务。上周新西兰奥克兰市也投票暂停其服务。Lime 承认是软件故障导致了这一问题，该公司声称受影响的滑板不到总数的 0.0045%。Lime 称初步的修正减少了事故发生数量，最终版更新预计将会更快完成。Lime 称，bug 存在于滑板

车的固件中，在极其罕见的情况下它会导致使用过程的过多刹车。这种罕见的情况通常是以最高速度下坡碰到路面坑洞或其它障碍物，前轮制动力过大，导致滑板车意外停止。

参考链接：https://www.solidot.org/story?sid=59675

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