国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 08 月 05 日-2019 年 08 月 11 日 **2019 年第 32 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 400 个，其中高危漏洞 62 个、中危漏洞 196 个、低危漏洞 142 个。漏洞平均分值为 5.0。本周收录的漏洞中，涉及 0day 漏洞 44 个（占 11%），其中互联网上出现“WordPress Email Subscribers&Newsletters 插件跨站脚本漏洞、Microsoft Windows PowerShell 命令执行漏洞”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 1923 个，与上周（2687 个）环比下降 28%。

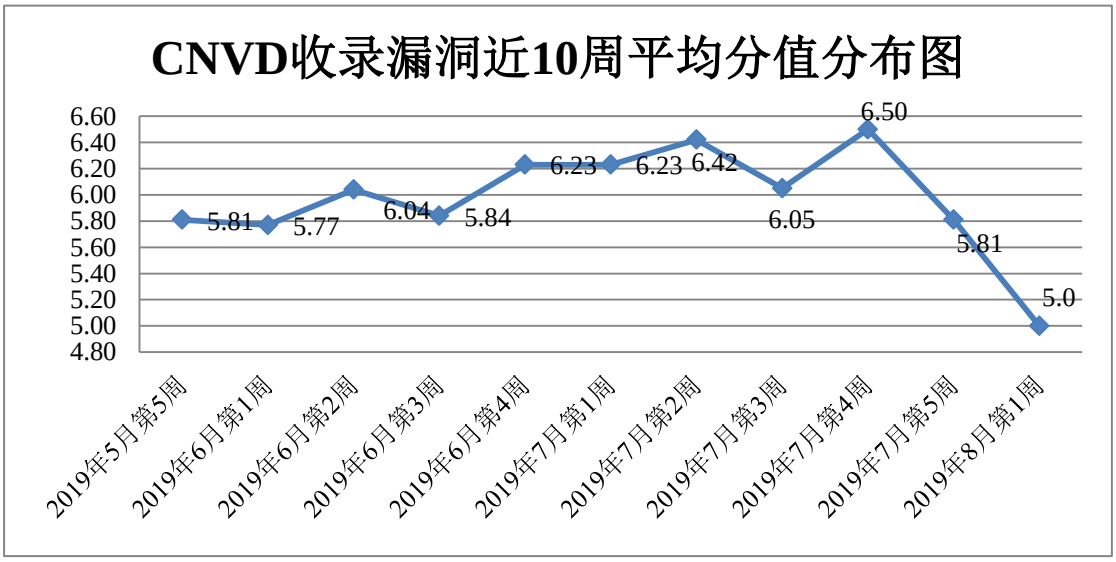

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向银行、保险、能源等重要行业单位通报漏洞事件 17 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 302 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 50 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40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：

上海卓卓网络科技有限公司、中铁十局第三建设有限公司、深圳龙兄弟数码锁有限公司、上海梦之路数字科技有限公司、南京新与力文化传播有限公司、哈尔滨优阳科技有限公司、上海泛微网络科技股份有限公司、重庆远秋科技有限公司、安徽省志鹄信息科技有限公司、淄博闪灵网络科技有限公司、广州商淘信息科技有限公司、南京品德科技有限责任公司、灵宝简好网络科技有限公司、深圳市迅雷网络技术有限公司、北京易勤信息技术有限公司、网展科技有限公司、北京正影网络科技有限公司、大同煤业金宇高岭土化工有限公司、漳州豆壳网络科技有限公司、广西集翔网大信息科技有限公司、上海汉得信息技术股份有限公司、横河电机(中国)有限公司、研华科技（中国）有限公司、酷溜网（北京）科技有限公司、镇江市云优网络科技有限公司、广州齐博网络科技有限公司、成都鹏博士电信传媒集团股份有限公司、重庆远秋科技公司、淄博闪灵网络科技有限公司、北京同城必应科技有限公司、多点新鲜（北京）电子商务有限公司、新疆雪莲花电子商务有限公司、深圳市杉川机器人有限公司、重庆冰炫科技有限公司、中国招标公共服务平台有限公司、哈尔滨新中新电子股份有限公司、四川久远银海软件股份有限公司、郑州狼烟网络科技、长沙市天心区斌网网络技术服务部、闻泰网络、合优网络、中国生态年会、中国人才研究会、中国企业联合会、中国水利电力质量管理协会、中国新闻传媒网、成都晚报社、熊海 CMS、海洋 CMS、Saxue、CMSWing、SaxueCMS 和 UCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、四川无声信息技术有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。新疆海狼科技有限公司、山东新潮信息技术有限公司、山东云天安全技术有限公司、南京众智维信息科技有限公司、内蒙古奥创科技有限公司、国网思极检测技术（北京）有限公司、长春嘉诚信息技术股份有限公司、北京铭图天成信息技术有限公司、国瑞数码零点实验室、山东华鲁科技发展股份有限公司、山石网科通信技术有限公司、北京小米科技有限责任公司、北京智游网安科技有限公司、山东云天安全大数据技术有限公司、广州非凡信息安全技术有限公司、成都市锐信安信息安全技术有限公司、河南信安世纪科技有限公司、上海物盾信息科技有限公司及其他个人白帽子向 CNVD 提交了 1923 件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1210 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）	763	763
奇安信网神（补天平台）	447	447
北京天融信网络安全技术有限公司	353	27
哈尔滨安天科技集团股份有限公司	289	0
华为技术有限公司	152	0
四川无声信息技术有限公司	87	87
深信服科技股份有限公司	79	1
北京神州绿盟科技有限公司	71	6
中国电信集团系统集成有限责任公司	61	0
新华三技术有限公司	56	0
恒安嘉新(北京)科技股份公司	50	1
北京数字观星科技有限公司	20	0
中新网络信息安全股份有限公司	11	11
北京知道创宇信息技术股份有限公司	7	2
南京联成科技发展股份有限公司	6	6
厦门服云信息科技有限公司	2	2
新疆海狼科技有限公司	60	60
山东新潮信息技术有限公司	57	57
山东云天安全技术有限公司	54	54
南京众智维信息科技有限公司	30	30
内蒙古奥创科技有限公司	24	24

国网思极检测技术（北京）有限公司	24	24
长春嘉诚信息技术股份有限公司	24	24
北京铭图天成信息技术有限公司	19	19
国瑞数码零点实验室	12	12
山东华鲁科技发展股份有限公司	7	7
山石网科通信技术有限公司	7	7
北京小米科技有限责任公司	2	2
北京智游网安科技有限公司	2	2
山东云天安全大数据技术有限公司	2	2
广州非凡信息安全技术有限公司	1	1
成都市锐信安信息安全技术有限公司	1	1
河南信安世纪科技有限公司	1	1
上海物盾信息科技有限公司	1	1
CNCERT 西藏分中心	6	6
CNCERT 贵州分中心	4	4
CNCERT 河北分中心	4	4
CNCERT 云南分中心	2	2
CNCERT 浙江分中心	1	1
个人	225	225
报送总计	3024	1923

本周漏洞按类型和厂商统计

本周，CNVD 收录了 400 个漏洞。应用程序 272 个，数据库 69 个，WEB 应用 42

个，网络设备（交换机、路由器等网络端设备）10 个，操作系统 6 个，安全产品 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	272
数据库	69
WEB 应用	42
网络设备（交换机、路由器等网络端设备）	10
操作系统	6
安全产品	1

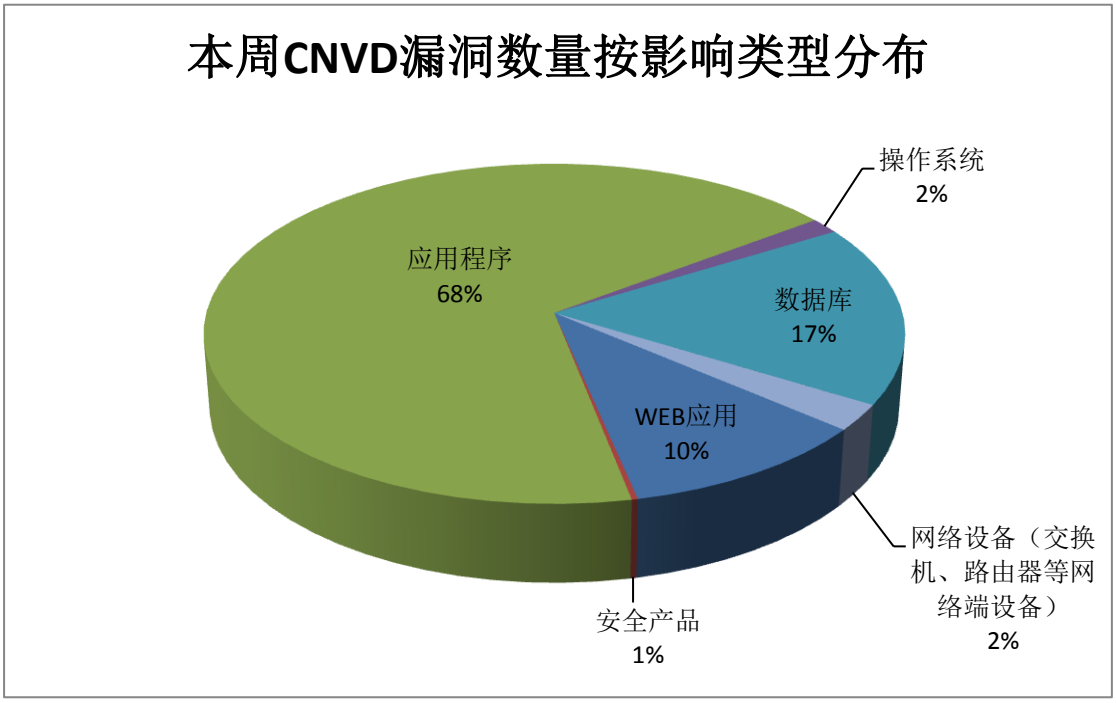

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、cPanel、Magento 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	Oracle	100	25%
2	cPanel	70	17%
3	Magento	44	11%
4	Adobe	25	6%
5	Intel	23	6%
6	Google	20	5%
7	CloudBees	18	5%

8	IBM	8	2%
9	Foo Labs	7	2%
10	其他	85	21%

本周行业漏洞收录情况

本周，CNVD 收录了 7 个电信行业漏洞，3 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“Siemens SIPROTEC 5 访问权限漏洞、DrayTek routers 跨站请求伪造漏洞、Cisco NX-OS Software 和 Cisco FXOS Software 命令注入漏洞”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/

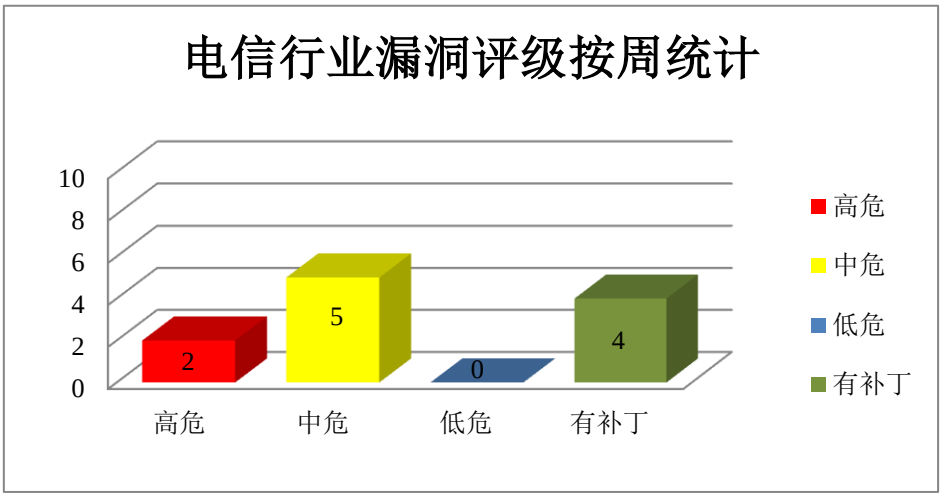

图 3 电信行业漏洞统计

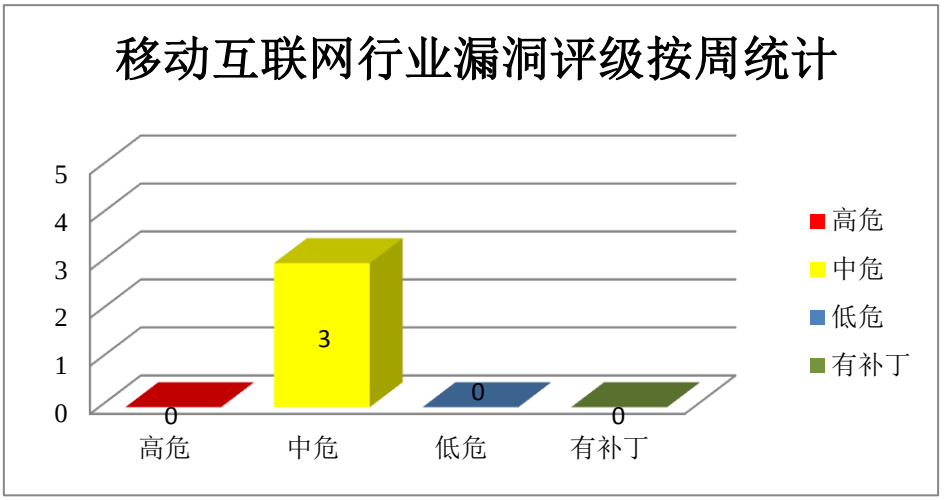

图 4 移动互联网行业漏洞统计

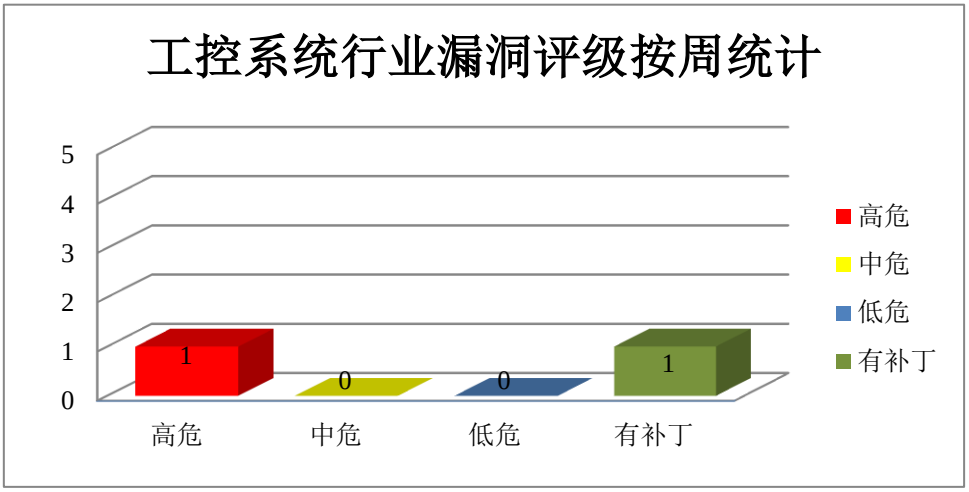

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle MySQL 是一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。本周，上述产品被披露存在访问控制错误漏洞，攻击者可利用漏洞造成拒绝服务（挂起或频繁崩溃）。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 访问控制错误漏洞（CNVD-2019-26706、CNVD-2019-26712、CNVD-2019-26710、CNVD-2019-26711、CNVD-2019-26713、CNVD-2019-26714、CNVD-2019-26715、CNVD-2019-26744）。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-2019-26706

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26712

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26710

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26711

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26713

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26714

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26715

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26744

2、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，该产品被披露存在内存错误引用漏洞，攻击者可利用

漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 内存错误引用漏洞（CNVD-2019-26034、CNVD-2019-26035、CNVD-2019-26036、CNVD-2019-26037、CNVD-2019-26038、CNVD-2019-26039、CNVD-2019-26040、CNVD-2019-26041）。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-2019-26034
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26035
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26036
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26037
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26038
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26039
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26040
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26041

3、Intel 产品安全漏洞

Intel Capability Licensing Service 是一款 Intel 功能许可服务接口。Intel Graphics Driver for Windows 是一款适用于 Windows 平台的显卡驱动程序。Intel Converged Security and Management Engine 是一款安全管理引擎。Intel TXE 是一款使用在 CPU（中央处理器）中具有硬件验证功能的信任执行引擎。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞逃离虚拟机，访问主机，提升权限，执行任意代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Intel Capability Licensing Service 权限提升漏洞、Intel Graphics Driver for Windows User Mode Driver 访问控制漏洞、Intel Graphics Driver for Windows Kernel Mode Driver 内存破坏漏洞、Intel Graphics Driver for Windows Kernel Mode Driver 任意代码执行漏洞（CNVD-2019-26185、CNVD-2019-26188）、Intel Converged Security and Management Engine 和 Intel TXE 缓冲区溢出漏洞、Intel Converged Security and Management Engine Intel AMT 任意代码执行漏洞、Intel Active Management Technology 拒绝服务漏洞。其中，“Intel Graphics Driver for Windows Kernel Mode Driver 内存破坏漏洞、Intel Graphics Driver for Windows Kernel Mode Driver 任意代码执行漏洞（CNVD-2019-26185、CNVD-2019-26188）、Intel Converged Security and Management Engine 和 Intel TXE 缓冲区溢出漏洞”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-2019-26169
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26173
http://www.cnvd.org.cn/flaw/show/CNVD-2019-26183

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26185

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26188

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26194

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26196

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26197

4、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信息泄露和安全绕过漏洞，攻击者可利用漏洞获取敏感信息，绕过安全限制，执行未授权的访问权限。

CNVD 收录的相关漏洞包括：Google Chrome 信息泄露漏洞（CNVD-2019-26205）、Google Chrome 安全绕过漏洞（CNVD-2019-26392、CNVD-2019-26403、CNVD-2019-26514、CNVD-2019-26517、CNVD-2019-26519、CNVD-2019-26520、CNVD-2019-26521）。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-2019-26205

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26392

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26403

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26514

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26517

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26519

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26520

http://www.cnvd.org.cn/flaw/show/CNVD-2019-26521

5、D-Link DVA-5592 信息泄露漏洞

D-Link DVA-5592 是一款无线路由器。本周，D-Link DVA-5592 被披露存在信息泄露漏洞。攻击者可利用该漏洞访问敏感信息（Wi-Fi 密码和电话号码）。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-2019-26657

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-2019-25803	Django SQL 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.djangoproject.com/weblog/2019/aug/01/security-releases/
CNVD-2019-25905	DrayTek routers 跨站请求伪造漏洞	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.draytek.com.au/blog/2018/05/23/security-alert-csrf-vulnerability-and-how-to-prevent-attacks/
CNVD-2019-25928	Siemens SIPROTEC 5 访问权限漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/pdf/ssa-632562.pdf
CNVD-2019-25972	libmodbus 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/stephane/libmodbus/commit/5ccdf5ef79d742640355d1132fa9e2abc7fbaefc
CNVD-2019-25986	SAP NetWeaver Process Integration 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=523994575
CNVD-2019-26202	Foxit PhantomPDF 缓冲区溢出漏洞	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.foxitsoftware.com/support/security-bulletins.php
CNVD-2019-26390	Apache Solr 远程代码执行漏洞（CNVD-2019-26390）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://issues.apache.org/jira/browse/SOLR-13669
CNVD-2019-26566	Linux kernel 缓冲区溢出漏洞（CNVD-2019-26566）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=1fa2337a315a2448c5434f41e00d56b01a22283c
CNVD-2019-26705	IBM Intelligent Operations Center XML 外部实体注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www-01.ibm.com/support/docview.wss?uid=ibm10956433
CNVD-2019-26763	ZeroMQ 堆栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://usn.ubuntu.com/4050-1/

小结：本周，Oracle 被披露存在访问控制错误漏洞，攻击者可利用漏洞造成拒绝服务（挂起或频繁崩溃）。此外，Adobe、Intel、Google 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，绕过安全限制，执行未授权的访问权限，提升权限，执行任意代码，造成拒绝服务等。D-Link DVA-5592 被披露存在信息泄露漏洞。攻击者可利用该漏洞访问敏感信息（Wi-Fi 密码和电话号码）。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 Email Subscribers&Newsletters 插件跨站脚本漏洞

验证描述

WordPress 是 WordPress 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。Email Subscribers&Newsletters 是使用在其中的一个新闻信息推送插件。

WordPress Email Subscribers&Newsletters 插件 4.1.6 版本中存在跨站脚本漏洞，攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://github.com/ivoschyk-cs/CVE-s/blob/master/Email%20Subscribers%20%26%20Newsletters%20Wordpress%20Plugin%20(XSS)

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-26567

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. WiFi WPA3 标准中发现新的 Dragonblood 漏洞

两位研究人员在 WiFi 联盟为设备供应商创建的安全建议中发现了两个新漏洞，允许攻击者从 WPA3 加密操作中泄漏信息并暴露出 WiFi 网络的密码。

参考链接：https://www.zdnet.com/article/new-dragonblood-vulnerabilities-found-in-wifi-wpa3-standard/

2. KDE 存在一个易于被利用的 0day 漏洞，影响广泛

安全研究员披露了 Linux KDE 桌面环境上存在的一个 0day 漏洞。此漏洞存在于 KDE v4 与 v5 版本中，该漏洞使得嵌入在.desktop 和.directory 文件中的命令在打开文件夹或者将压缩文件夹提取到桌面时即可执行，目前几乎所有 Linux 发行版都在使用易受攻击的 KDE 版本。

参考链接：https://www.bleepingcomputer.com/news/security/zero-day-bug-in-kde-4-5-executes-commands-by-opening-a-folder/

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