国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 11 月 11 日-2019 年 11 月 17 日　　2019 年第 46 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 541 个，其中高危漏洞 142 个、中危漏洞 334 个、低危漏洞 65 个。漏洞平均分值为 5.67。本周收录的漏洞中，涉及 0day 漏洞 212 个（占 39%），其中互联网上出现“TP-LINK TL-WR940N 和 TL-WR941ND 缓冲区溢出漏洞、Belkin Linksys EA6500 路径遍历漏洞”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 3140 个，与上周（7452 个）环比减少 58%。

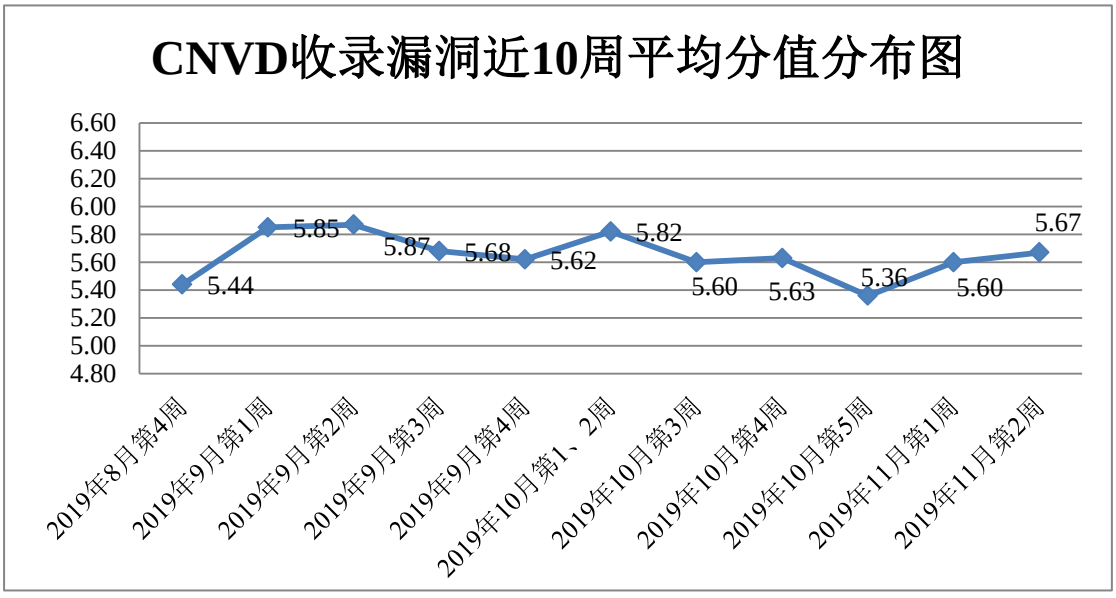

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 18 起，向基础电信企业通报漏洞事件 4 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 335 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 35 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 20 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：

上海卓岚信息科技有限公司、洛阳云业信息科技有限公司、昆明云涛科技有限公司、惠州市众兴互联科技有限公司、北京世纪长秋科技有限公司、深圳市蓝色航线科技有限公司、北京易勤信息技术有限公司、南京品德科技有限责任公司、中控智慧科技股份有限公司、湖南壹拾捌号网络技术有限公司、深圳市海洋蓝科技有限公司、长沙米拓信息技术有限公司、上海师廉网络科技发展有限公司、苏州天汇信息技术有限公司、上海泛微网络科技股份有限公司、浙江禾连网络科技有限公司、淄博闪灵网络科技有限公司、北京翰博尔信息技术股份有限公司、北京京东世纪贸易有限公司、湖南心艾网络科技有限公司、三五互联科技股份有限公司、广联达科技股份有限公司、北京智信数图科技有限公司、普联技术有限公司、四平市九州易通科技有限公司、秦皇岛市五六七七零网络科技有限公司、安徽小皮教育科技有限公司、广州万户网络技术有限公司、青岛易软天创网络科技有限公司、北京小米科技有限责任公司、成都百都科技有限公司、合肥明靖信息科技有限公司、研华科技（中国）有限公司、沧州市凡诺广告传媒有限公司、珠海玖时光科技有限公司、杭州海康威视数字技术股份有限公司、上海商创网络科技有限公司、广州凌科普华网络科技有限公司、西安瑞友信息技术资讯有限公司、广州恒企教育科技有限公司、廊坊市极致网络科技有限公司、上海万欣计算机信息科技有限公司、咪咕视讯科技有限公司、北京爱奇艺科技有限公司、北京快手科技有限公司、泰安梦泰尔软件有限公司、北京风行在线技术有限公司、沈阳市皇姑区爱浓网络技术服务中心、中国航空制造技术研究院、安徽启明星工作室、雷风影视、睿谷信息科技、MyuCMS 社区、5iSNS 实验室、海洋 CMS、苹果 CMS、梦雨 cms、超级 cms、UQCMS、MyuCMS、PHPEMS、ThinkCMF 和 XYCMS。

本周，CNVD 发布了《Microsoft 发布 2019 年 11 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5285

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、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、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。远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、山东云天安全技术有限公司、山东新潮信息技术有限公司、

内蒙古奥创科技有限公司、北京铭图天成信息技术有限公司、任子行网络技术股份有限公司、南京众智维信息科技有限公司、杭州海康威视数字技术股份有限公司、北京华云安信息技术有限公司、安徽智云信息安全有限公司、广州蕴辰网络科技有限公司、北京君信安科技有限公司、山东华鲁科技发展股份有限公司、雷石安全实验室、国家互联网应急中心、江苏保旺达软件技术有限公司、北京智游网安科技有限公司、杭州迪普科技股份有限公司、成都安美勤信息技术股份有限公司、河南灵创电子科技有限公司、河南信安世纪科技有限公司、亨通工控安全研究院有限公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 3140 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 2433 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）	1072	1072
奇安信网神（补天平台）	966	966
上海交大	395	395
阿里云计算有限公司	481	1
北京天融信网络安全技术有限公司	324	1
哈尔滨安天科技集团股份有限公司	216	0
华为技术有限公司	112	0
深信服科技股份有限公司	111	2
北京神州绿盟科技有限公司	100	0
北京启明星辰信息安全技术有限公司	55	11
恒安嘉新(北京)科技股份公司	53	0
新华三技术有限公司	33	0
浙江大华技术股份有限公司	20	20
北京数字观星科技有限公司	19	0
四川无声信息技术有限公	12	12

司		
中新网络信息安全股份有限公司	9	9
北京知道创宇信息技术股份有限公司	8	2
厦门服云信息科技有限公司	3	3
南京联成科技发展股份有限公司	2	2
中国电信集团系统集成有限责任公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	68	68
国瑞数码零点实验室	60	60
山东云天安全技术有限公司	36	36
山东新潮信息技术有限公司	36	36
内蒙古奥创科技有限公司	34	34
北京铭图天成信息技术有限公司	31	31
任子行网络技术股份有限公司	20	20
南京众智维信息科技有限公司	19	19
杭州海康威视数字技术股份有限公司	14	14
北京华云安信息技术有限公司	13	13
安徽智云信息安全有限公司	10	10
广州蕴辰网络科技有限公司	6	6
北京君信安科技有限公司	5	5
山东华鲁科技发展股份有限公司	4	4
雷石安全实验室	4	4
国家互联网应急中心	2	2

江苏保旺达软件技术有限公司	2	2
北京智游网安科技有限公司	2	2
杭州迪普科技股份有限公司	2	2
成都安美勤信息技术股份有限公司	1	1
河南灵创电子科技有限公司	1	1
河南信安世纪科技有限公司	1	1
亨通工控安全研究院有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 宁夏分中心	2	2
CNCERT 西藏分中心	2	2
CNCERT 贵州分中心	1	1
个人	265	265
报送总计	4635	3140

本周漏洞按类型和厂商统计

本周，CNVD 收录了 541 个漏洞。应用程序 295 个，WEB 应用 160 个，操作系统 58 个，网络设备（交换机、路由器等网络端设备）21 个，安全产品 3 个，数据库 2 个，智能设备（物联网终端设备）2 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	295
WEB 应用	160
操作系统	58
网络设备（交换机、路由器等网络端设备）	21
安全产品	3
数据库	2
智能设备（物联网终端设备）漏洞	2

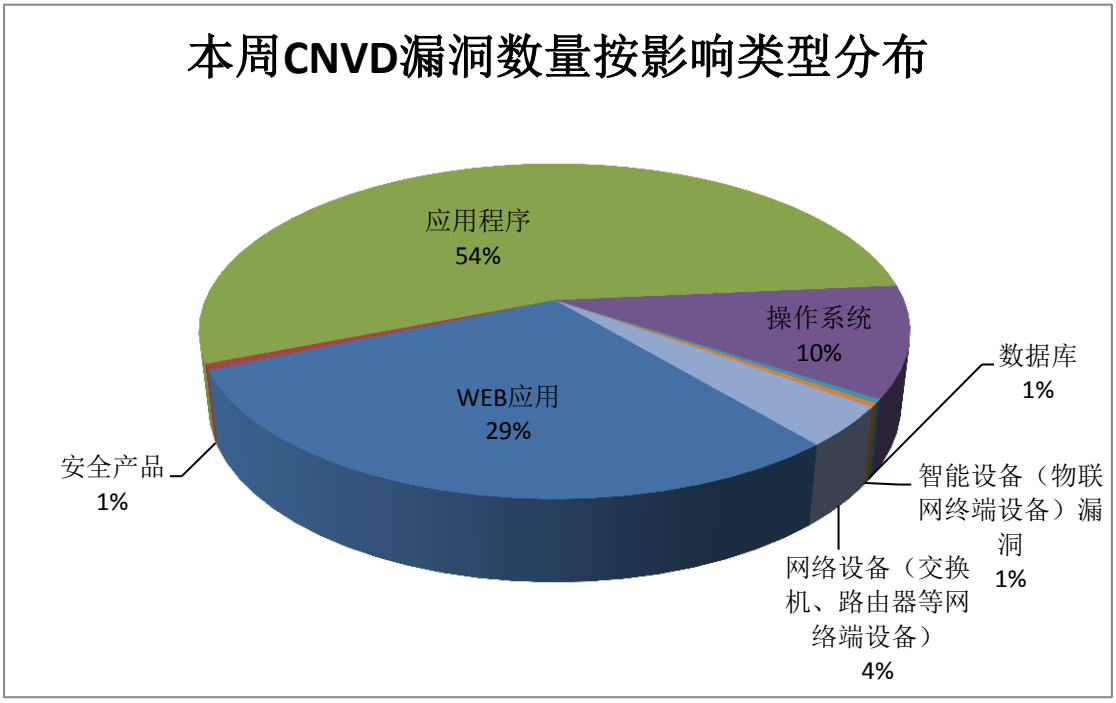

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Magento、Google、Oracle 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	Magento	51	10%
2	Google	45	9%
3	Oracle	38	7%
4	淄博闪灵网络科技有限公司	17	3%
5	JetBrains	13	2%
6	Cryptocat	13	2%
7	Microsoft	12	2%
8	IBM	11	2%
9	Linux	10	2%
10	其他	331	61%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，47 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“IBM DB2 缓冲区溢出漏洞（CNVD-2019-40603）、TP-Link TL-WDR4300 跨站请求伪造漏洞（CNVD-2019-40473）、Siemens SIMATIC S7-12

00 CPU 访问漏洞、Google Android Media Framework 拒绝服务漏洞（CNVD-2019-40055）”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，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/

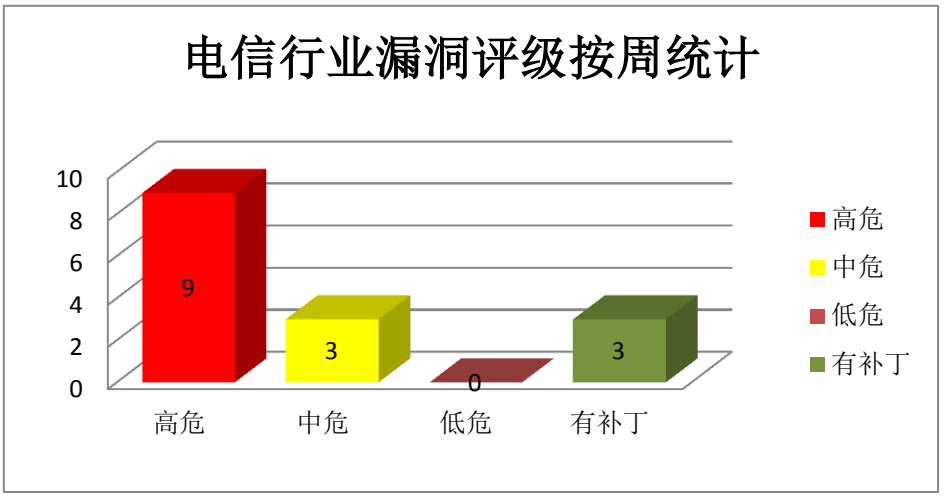

图 3 电信行业漏洞统计

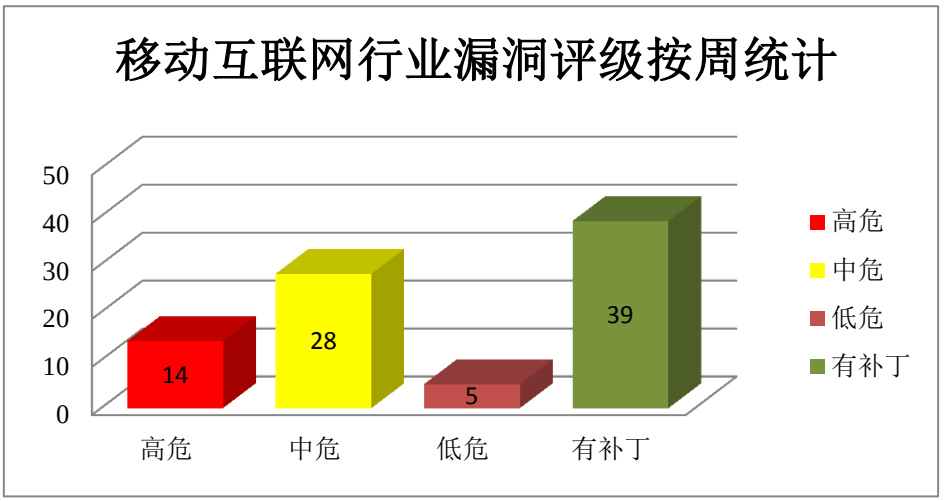

图 4 移动互联网行业漏洞统计

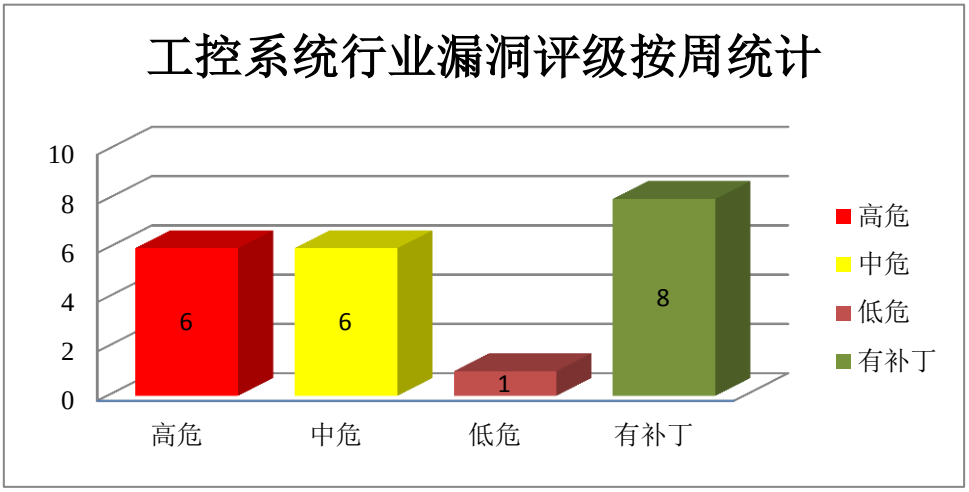

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。V8 是其中的一套开源 JavaScript 引擎。Android 是一套以 Linux 为基础的开源操作系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限、造成拒绝服务和缓冲区溢出。

CNVD 收录的相关漏洞包括：Google Chrome V8 远程代码执行漏洞（CNVD-2019-40080）、Google Chrome 拒绝服务漏洞（CNVD-2019-40126）、Google Chrome audio 组件资源管理错误漏洞、Google Chrome PDFium 资源管理错误漏洞（CNVD-2019-40305）、Google Android Kernel 组件权限提升漏洞（CNVD-2019-40503、CNVD-2019-40504）、Google Chrome V8 缓冲区溢出漏洞（CNVD-2019-41021）、Google Android 权限许可和访问控制漏洞（CNVD-2019-41024）。其中，除“Google Android 权限许可和访问控制漏洞（CNVD-2019-41024）、Google Chrome audio 组件资源管理错误漏洞、Google Chrome 拒绝服务漏洞（CNVD-2019-40126）”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-2019-40080

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40126

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40304

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40305

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40503

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40504

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41021

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41024

2、IBM 产品安全漏洞

IBM InfoSphere Information Server 是美国 IBM 公司的一套数据整合平台。IBM Cognos Analytics 是一套商业智能软件。IBM Spectrum Scale 是一套基于 IBM GPFS（专为 PB 级存储管理而优化的企业文件管理系统）的可扩展的数据及文件管理解决方案。IBM Workload Scheduler Distributed 是一套企业任务调度软件。IBM DB2 是一套关系型数据库管理系统。IBM QRadar SIEM 是一套利用安全智能保护资产和信息远离高级威胁的解决方案。IBM Security Identity Manager 是一种基于策略的自动化解决方案。IBM Sterling Connect:Express for UNIX 是一套适用于 UNIX 平台的文件传输解决方案。FTP Server 是其中的一个 FTP（文件传输协议）解析器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，获取 root 权限或造成拒绝服务等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 跨站请求伪造漏洞（CNVD-2019-40094）、IBM Cognos Analytics 跨站脚本漏洞（CNVD-2019-40462）、IBM Spectrum Scale 权限提升漏洞、IBM Workload Scheduler Distributed 权限提升漏洞、IBM DB2 缓冲区溢出漏洞（CNVD-2019-40603）、IBM QRadar SIEM 跨站脚本漏洞（CNVD-2019-40708）、IBM Security Identity Manager XML 外部实体注入漏洞、IBM SterlinIBM Sterling Connect:Express for UNIX FTP Server 缓冲区溢出漏洞。其中，除“IBM InfoSphere Information Server 跨站请求伪造漏洞（CNVD-2019-40094）、IBM Cognos Analytics 跨站脚本漏洞（CNVD-2019-40462）、IBM QRadar SIEM 跨站脚本漏洞（CNVD-2019-40708）、IBM Security Identity Manager XML 外部实体注入漏洞”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-2019-40094

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40462

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40570

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40571

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40603

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40708

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40822

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40898

3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。Linux Vserver 是一款基于 Linux 的虚拟专用服务器实现。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行非法操作或导致拒绝服务。

CNVD 收录的相关漏洞包括：Linux kernel 内存泄漏漏洞（CNVD-2019-40135、CNVD-2019-40151、CNVD-2019-40152、CNVD-2019-40153、CNVD-2019-40156、CNVD-2019-40157）、Linux kernel 输入验证错误漏洞（CNVD-2019-40470）、Linux Vserver 权限提升漏洞。其中，除“Linux kernel 内存泄漏漏洞（CNVD-2019-40153）”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-2019-40135
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40151
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40152
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40153
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40156
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40157
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40470
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40471

4、Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Microsoft Outlook 是一款个人信息管理系统软件。Microsoft Word 是一套 Office 套件中的文字处理软件。Microsoft Dynamics 365 是一套适用于跨国企业的 ERP 业务解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限等。

CNVD 收录的相关漏洞包括：Microsoft Outlook 权限提升漏洞（CNVD-2019-40535）、Microsoft Outlook 远程代码执行漏洞（CNVD-2019-40556）、Microsoft Outlook 内存破坏漏洞（CNVD-2019-40557）、Microsoft Word 远程代码执行漏洞（CNVD-2019-40537、CNVD-2019-40558）、Microsoft Windows DHCP 远程代码执行漏洞、Microsoft Dynamics On-Premise 权限提升漏洞、Microsoft Windows NTFS 权限提升漏洞（CNVD-2019-40566）。其中，除“Microsoft Outlook 权限提升漏洞（CNVD-2019-40535）、Microsoft Dynamics On-Premise 权限提升漏洞”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-2019-40535
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40537
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40556
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40557
http://www.cnvd.org.cn/flaw/show/CNVD-2019-40558

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40564

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40565

http://www.cnvd.org.cn/flaw/show/CNVD-2019-40566

5、Apache Flink 任意 Jar 包上传导致远程代码执行漏洞

Apache Flink 是由 Apache 软件基金会开发的开源流处理框架，其核心是用 Java 和 Scala 编写的分布式流数据流引擎。Flink 以数据并行和流水线方式执行任意流数据程序，Flink 的流水线运行时系统可以执行批处理和流处理程序。本周，Apache Flink 被披露存在远程代码执行漏洞。攻击者可利用该漏洞在 Apache Flink Dashboard 页面中上传任意 Jar 包，利用 Metasploit 在 Apache Flink 服务器中执行任意代码。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-2019-40563

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-2019-39943	Fortinet FortiExtender 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-19-273
CNVD-2019-40065	Milesight IP security cameras 授权问题漏洞	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.milesight.com
CNVD-2019-40096	Red Hat OpenShift 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.openshift.com
CNVD-2019-40147	Citrix Systems SD-WAN Center 和 NetScaler SD-WAN Center 命令注入漏洞（CNVD-2019-40147）	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.citrix.com/article/CTX251987
CNVD-2019-40473	TP-Link TL-WDR4300 跨站请求伪造漏洞（CNVD-2019-40473）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tp-link.com
CNVD-2019-40477	NVIDIA Windows GPU Display Driver 空指针解引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://nvidia.custhelp.com/app/answers/detail/a_id/4907
CNVD-2019-40595	JetBrains Toolbox 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://blog.jetbrains.com/blog/2019/10/

			29/jetbrains-security-bulletin-q3-2019/
CNVD-2019-40759	Magento 远程代码执行漏洞（CNVD-2019-40759）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://magento.com/security/patches/magento-2.3.3-and-2.2.10-security-update
CNVD-2019-40826	Micronet INplc-RT 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：http://www.mnc.co.jp/INplc/info_20180907_E.htm
CNVD-2019-40150	Citrix Systems SD-WAN Center 和 NetScaler SD-WAN Center 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://support.citrix.com/article/CTX251987

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限、造成拒绝服务和缓冲区溢出。此外，IBM、Linux、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，提升权限或造成拒绝服务等。另外，Apache Flink 被披露存在远程代码执行漏洞。攻击者可利用该漏洞在 Apache Flink Dashboard 页面中上传任意 Jar 包，利用 Metasploit 在 Apache Flink 服务器中执行任意代码。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、TP-LINK TL-WR940N 和 TL-WR941ND 缓冲区溢出漏洞

验证描述

TP-Link TL-WR940N 和 TP-Link TL-WR941ND 都是中国普联（TP-Link）的一款无线路由器。

TP-LINK TL-WR940N 和 TL-WR941ND 中存在缓冲区溢出漏洞，攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

验证信息

POC 链接：https://packetstormsecurity.com/files/152458/TP-LINK-TL-WR940N-TL-WR941ND-Buffer-Overflow.html

参考链接： https://www.cnvd.org.cn/flaw/show/CNVD-2019-40472

信息提供者

北京天融信网络安全技术有限公司

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. WhatsApp 存在漏洞可被利用安装间谍软件

WhatsApp 最近修复了一个严重漏洞，即 CVE-2019-11931，该漏洞可能使攻击者秘密安装间谍软件，远程破坏目标设备。该漏洞影响 Google Android，Apple iOS 和 Microsoft Windows 的 WhatsApp 版本。

参考链接：https://securityaffairs.co/wordpress/93932/hacking/whatsapp-flaw-cve-2019-11931.html

2. RHEL 和 CentOS 再获重要内核安全更新：缓解英特尔处理器漏洞影响

Red Hat 和 CentOS 宣布了适用于 Red Hat Enterprise Linux 6/7、以及 CentOS Linux 6/7 操作系统分支的重要内核安全更新。本次内核安全更新主要针对最新曝光的英特尔 CPU 微架构漏洞，修复了 ZombieLoad v2 漏洞以及其他问题。CentOS 社区也移植该更新到 CentOS Linux 6/7 上。

参考链接：https://www.cnbeta.com/articles/tech/911581.htm

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