国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 12 月 16 日-2019 年 12 月 22 日 **2019 年第 51 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 230 个，其中高危漏洞 77 个、中危漏洞 122 个、低危漏洞 31 个。漏洞平均分值为 5.86。本周收录的漏洞中，涉及 0day 漏洞 51 个（占 22%），其中互联网上出现“Max Secure Anti Virus Plus 权限提升漏洞、NAPC Xinet Elegant 6 Asset Library Web Interface SQL 注入漏洞”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 3156 个，与上周（2695 个）环比增长 17%。

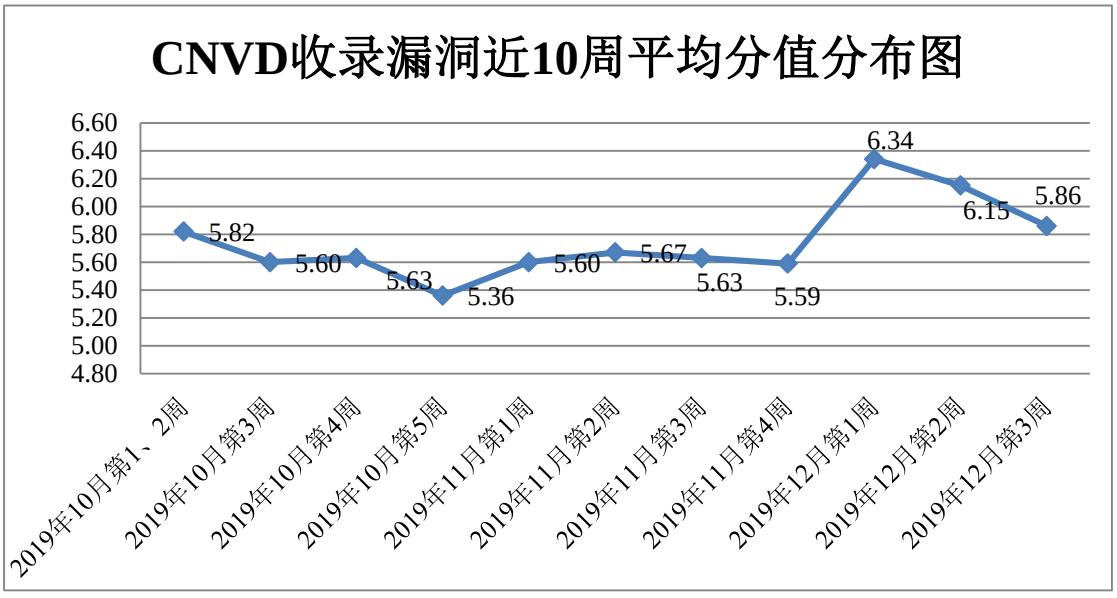

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 29 起，向基础电信企业通报漏洞事件 7 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 222 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 22 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 23 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：

上海彩圣信息科技有限公司、郑州金特莱电子有限公司、酷艺文化网络科技有限公司、厦门才茂通信科技有限公司、湖南翱云网络科技有限公司、广州齐博网络科技有限公司、广州永拓信息科技有限公司、湖北淘码千维信息科技有限公司、江西金磊科技发展有限公司、南京软核科技有限公司、江苏金智科技股份有限公司、国电南京自动化股份有限公司、金山软件股份有限公司、廊坊市极致网络科技有限公司、北京万户网络技术有限公司、镇江市云优网络科技有限公司、深圳市迪元素科技有限公司、海南赞赞网络科技有限公司、长沙德尚网络科技有限公司、睿谷信息科技有限公司、上海商派网络科技有限公司、法治中国普法教育工作办公室、台湾威岦網頁設計有限公司、中企动力科技股份有限公司、北京超越无限信息技术有限公司、昆明云涛科技有限公司、成都鹏博士电信传媒集团股份有限公司、思源电气股份有限公司、深圳国网南瑞科技有限公司、南京南瑞继保电气有限公司、北京邦永科技有限公司、重庆猫扑网络科技有限公司、帆软软件有限公司、上海商创网络科技有限公司、北京得安信息技术有限公司、广州合优网络科技有限公司、陕西公众软件有限公司、景騰多媒體股份有限公司、南大傲拓科技江苏股份有限公司、无锡信捷电气股份有限公司、山西临猗农村商业银行股份有限公司、深圳搜豹网络有限公司、青岛易软天创网络科技有限公司、德派软件（北京）有限公司、北京良精志诚科技有限责任公司、苏州恩斯特网络科技有限公司、太原飞扬动力科技有限公司上海艺觉网络科技有限公司、洛阳云业信息科技有限公司、南昌市驰硕网络科技有限公司、南京磐能电力科技股份有限公司、武汉中元华电科技股份有限公司、长园深瑞继保自动化有限公司、山东科汇电力自动化股份有限公司、武汉方德机器人科技有限公司、推券客联盟、帝国软件、玛塔留言板、袁志蒙工作室、海洋 CMS、MyuCMS 社区、Zzzcms、UQCMS、Scikit-Learn、TuziCMS 和 Nsasoft US。

本周，CNVD 发布了《关于 Chrome 浏览器 WebSQL 和 SQLite 存在任意代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5333

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、中新网络信息安全股份有限公司、华为技术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、内蒙古奥创科技有限公司、内蒙古洞明科技有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司、杭州海康威视数字技术股份有限公司、国瑞数码零点实验室、山东云天安全技术有限公司、河南信安世纪科技有限公司、北京圣博润高新技术股份有限公司、北京网思科平科技有限公司、山石网科通信技术股份有限公司、北京云科安信科技有限公司、广州万方计算机科技有限公司、北京智游网安科技有限公司、北京信联科汇科技有限公司、山东华鲁科技发展股份有限公司、上海并擎软件科技有限公司、上海端御信息科技有限公司、杭州迪普科技股份有限公司及其他个人白帽子向 CNVD 提交了 3156 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 2178 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
奇安信网神（补天平台）	1011	1011
斗象科技（漏洞盒子）	715	715
阿里云计算有限公司	461	0
上海交大	452	452
北京天融信网络安全技术有限公司	234	11
哈尔滨安天科技集团股份有限公司	207	0
中新网络信息安全股份有限公司	154	154
华为技术有限公司	125	0
北京神州绿盟科技有限公司	112	2
新华三技术有限公司	88	0
恒安嘉新(北京)科技股份公司	82	0
深信服科技股份有限公司	73	3
北京启明星辰信息安全技术有限公司	58	1
厦门服云信息科技有限公司	46	0
北京数字观星科技有限公	20	0

司		
深圳市腾讯计算机系统有限公司（玄武实验室）	14	14
北京知道创宇信息技术股份有限公司	4	1
沈阳东软系统集成工程有限公司	2	2
南京联成科技发展股份有限公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	155	155
内蒙古奥创科技有限公司	64	64
内蒙古洞明科技有限公司	52	52
山东新潮信息技术有限公司	36	36
河南灵创电子科技有限公司	20	20
杭州海康威视数字技术股份有限公司	19	19
国瑞数码零点实验室	15	15
杭州迪普科技股份有限公司	14	0
山东云天安全技术有限公司	7	7
河南信安世纪科技有限公司	5	5
北京圣博润高新技术股份有限公司	3	3
北京网思科平科技有限公司	3	3
山石网科通信技术股份有限公司	3	3
北京云科安信科技有限公司	2	2
广州万方计算机科技有限公司	2	2
北京智游网安科技有限公司	1	1
北京信联科汇科技有限公司	1	1

山东华鲁科技发展股份有限公司	1	1
上海并擎软件科技有限公司	1	1
上海端御信息科技有限公司	1	1
CNCERT 宁夏分中心	11	11
CNCERT 贵州分中心	4	4
CNCERT 甘肃分中心	2	2
CNCERT 天津分中心	2	2
个人	379	379
报送总计	4662	3156

本周漏洞按类型和厂商统计

本周，CNVD 收录了 230 个漏洞。应用程序 135 个，操作系统 61 个，网络设备（交换机、路由器等网络端设备）12 个，智能设备（物联网终端设备）12 个，WEB 应用 8 个，安全产品 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	135
操作系统	61
网络设备（交换机、路由器等网络端设备）	12
智能设备（物联网终端设备）	12
WEB 应用	8
安全产品	2

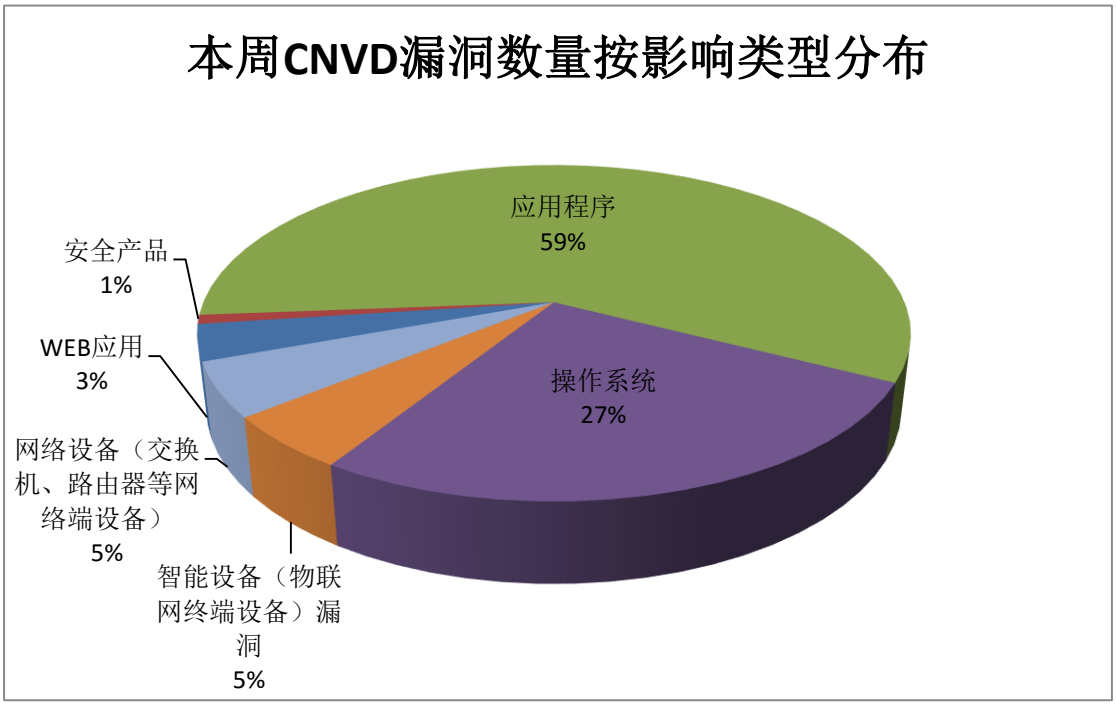

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Google、Apple 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	Siemens	41	18%
2	Google	25	11%
3	Apple	22	10%
4	Adobe	16	7%
5	Linux	16	7%
6	Microsoft	10	4%
7	CloudBees	9	4%
8	Oracle	9	4%
9	Cisco	7	3%
10	其他	75	32%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，37 个移动互联网行业漏洞，48 个工控行业漏洞（如下图所示）。其中，“TP-Link TL-WR841N 缓冲区溢出漏洞、Cisco IOS 和 IOS XE IP Ident 拒绝服务漏洞、Siemens SPPA-T3000 MS3000 Migration Server 堆缓冲

区溢出漏洞、Google Android NFC 组件权限许可和访问控制漏洞、多款 Apple 产品 WebKit 组件资源管理错误漏洞、Advantech WebAccess 缓冲区溢出漏洞（CNVD-2019-45387）”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/

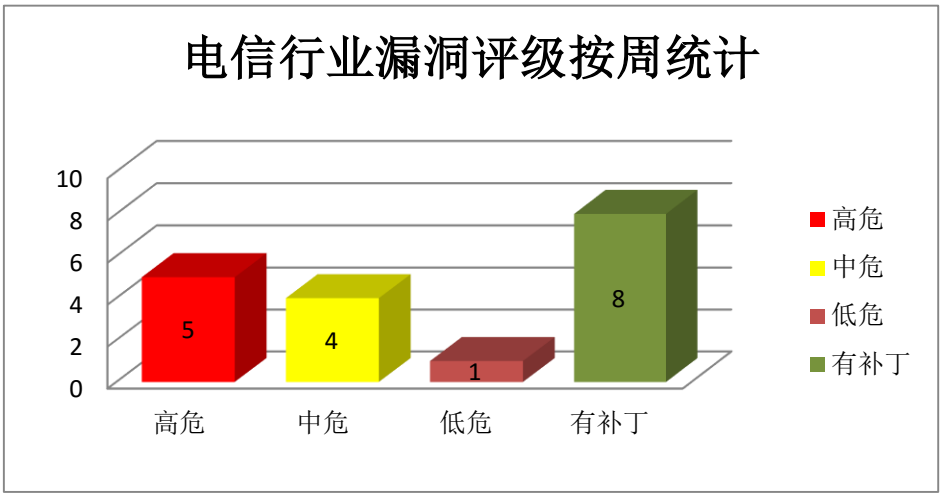

图 3 电信行业漏洞统计

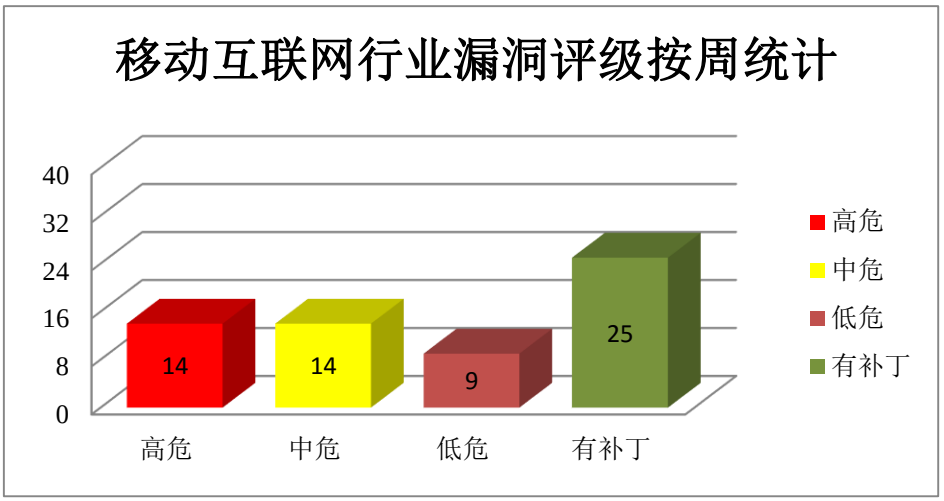

图 4 移动互联网行业漏洞统计

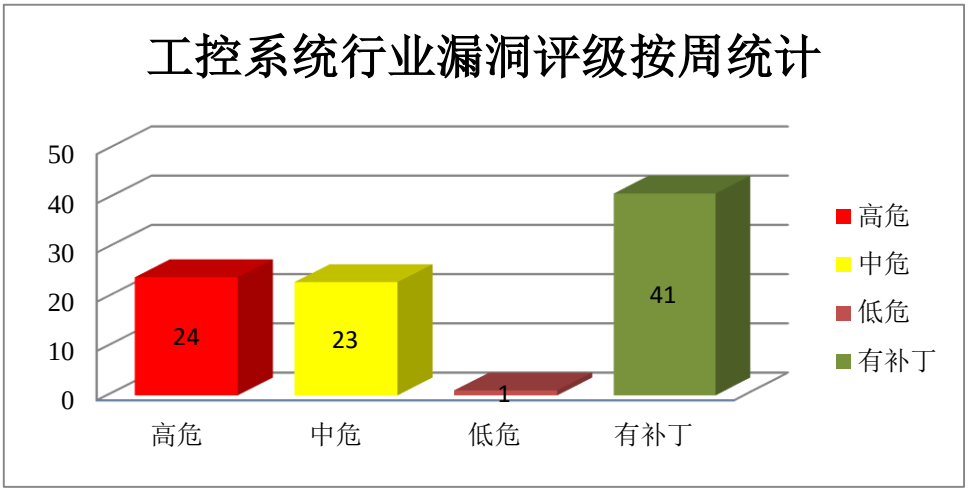

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。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 Windows 7 SP1 是一款操作系统。Microsoft Windows XP 是一套 PC 和平板电脑使用的操作系统。Remote Desktop Protocol 是一个远程桌面协议。Microsoft SharePoint 是一套企业业务协作平台。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，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-45913）、Microsoft Windows 和 Microsoft Windows Server 提权漏洞（CNVD-2019-45911）、Microsoft Windows 和 Microsoft Windows Server OLE 远程代码执行漏洞、Microsoft Windows Remote Desktop Protocol 信息泄露漏洞、Microsoft Windows Media Player 信息泄露漏洞（CNVD-2019-45916）、Microsoft Windows Graphics Device Interface 信息泄露漏洞（CNVD-2019-45917）、Microsoft Windows Media Player 信息泄露漏洞（CNVD-2019-45918）、Microsoft SharePoint Server 信息泄露漏洞（CNVD-2019-46110）。其中，“Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-45913）、Microsoft Windows 和 Microsoft Windows Server 提权漏洞（CNVD-2019-45911）”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-2019-45913

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45911

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45914

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45915

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45916

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45917

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45918

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46110

2、Siemens 产品安全漏洞

SPPA-T3000 是一种分布式控制系统，主要应用于火力发电厂和大型可再生能源发电厂。MS3000 Migration Server 是其中的一个迁移服务器。本周，上述产品被披露存在堆缓冲区溢出漏洞，攻击者可利用漏洞获得 root 权限，导致拒绝服务并执行任意代码。

CNVD 收录的相关漏洞包括：Siemens SPPA-T3000 MS3000 Migration Server 堆缓冲区溢出漏洞（CNVD-2019-45378、CNVD-2019-45409、CNVD-2019-45410、CNVD-2019-45411、CNVD-2019-45417、CNVD-2019-45418、CNVD-2019-45419、CNVD-2019-45421）。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-2019-45378

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45409

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45410

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45411

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45417

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45418

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45419

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45421

3、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。Adobe Photoshop 是一套图片处理软件。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。

CNVD 收录的相关漏洞包括：Adobe Photoshop CC 内存破坏漏洞（CNVD-2019-45962、CNVD-2019-45969）、Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2019-45967）、Adobe Acrobat 和 Reader 内存错误引用漏洞（CNVD-2019-45970、CNVD-2019-45971、CNVD-2019-45973、CNVD-2019-45974、CNVD-2019-45975）。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-2019-45962

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45967

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45969

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45970

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45971

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45973

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45974

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45975

4、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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致拒绝服务，释放后重用。

CNVD 收录的相关漏洞包括：Linux kernel 内存错误引用漏洞（CNVD-2019-45875、CNVD-2019-45876、CNVD-2019-45877、CNVD-2019-45878、CNVD-2019-45879、CNVD-2019-45906、CNVD-2019-45907）、Linux kernel 缓冲区溢出漏洞（CNVD-2019-45882）。其中，“Linux kernel 缓冲区溢出漏洞（CNVD-2019-45882）”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-2019-45875

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45876

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45877

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45878

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45879

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45882

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45906

http://www.cnvd.org.cn/flaw/show/CNVD-2019-45907

5、Red Hat FreeIPA 缓冲区溢出漏洞

Red Hat FreeIPA 是一套集成的安全信息管理解决方案。本周，Red Hat FreeIPA 被披露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。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-2019-46410

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-2019-45387	Advantech WebAccess 缓冲区溢出漏洞（CNVD-2019-45387）	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.advantech.com
CNVD-2019-45610	WordPress Beaver Builder 和 Elementor 插件身份验证绕过	高	厂商已发布了漏洞修复程序，请及时关注更新：

	漏洞		https://wordpress.org
CNVD-2019-45891	Google Android Qualcomm DSP_Services 组件缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2018-11-01
CNVD-2019-45900	WordPress quiz-master-next 跨站脚本漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wordpress.org/plugins/quiz-master-next/#developers
CNVD-2019-46109	Mozilla Network Security Services 缓冲区溢出漏洞	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://github.com/nss-dev/nss
CNVD-2019-46122	多款 Apple 产品 WebKit 组件资源管理错误漏洞	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.apple.com/en-us/HT210785
CNVD-2019-46129	Apple Xcode ld64 组件缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/en-us/HT210796
CNVD-2019-46266	TP-Link Archer 路由器未认证访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://static.tp-link.com/2019/201909/20190917/Archer_C5v4190815.rar
CNVD-2019-46404	libnbd 输入验证错误漏洞	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://github.com/libguestfs/libnbd
CNVD-2019-46435	Cisco IOS 和 IOS XE IP Ident 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-identd-dos

小结：本周，Microsoft 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，提升权限，执行任意代码。此外，Siemens、Adobe、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获得 root 权限，导致拒绝服务并执行任意代码等。另外，Red Hat FreeIPA 被披露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。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、Max Secure Anti Virus Plus 权限提升漏洞

验证描述

Max Secure Software Anti Virus Plus 是印度 Max Secure Software 公司的一套杀毒软件。

Max Secure Software Anti Virus Plus 19.0.4.020 版本中存在安全漏洞。攻击者可利用该漏洞替换.exe 或.dll 文件，提升权限。

验证信息

POC 链接：https://packetstormsecurity.com/files/155506/Max-Secure-Anti-Virus-Plus-19.0.4.020-Insecure-Permissions.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2019-46105

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. TP-Link Archer 系列路由器漏洞可使 Admin 账户密码保护失效

TP-Link Archer C5（v4）路由器中存在固件漏洞。远程攻击者可以通过局域网（LAN）上的 Telnet 来控制路由器的配置，并通过 LAN 或广域网（WAN）连接到文件传输协议（FTP）服务器。该缺陷可以授予未经授权的第三方使用管理员特权访问路由器，而这是所有用户在该设备上的默认设置，而无需进行适当的身份验证。在使用此类路由器启用访客 Wi-Fi 的商业网络上，风险更大。如果将其放置在企业网络上，则受损的路由器可能成为攻击者的切入点，并且成为侦察和横向移动策略中枢转的场所。

参考链接：https://www.freebuf.com/vuls/223076.html

2. 新的 WhatsApp 漏洞使群组聊天崩溃，永久删除历史记录

以色列 NSO Group-Pegasus 通过 WhatsApp 进行侦听，安全研究人员表示，他们已经在 WhatsApp 中检测到一个漏洞，一旦黑客在聊天中引入破坏性消息，该漏洞便会导致群聊崩溃，整个群组聊天记录将被永久删除。

参考链接：https://cio.economictimes.indiatimes.com/news/digital-security/new-whatsapp-bug-crashes-group-chat-deletes-history-forever/72864383

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