国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 09 月 23 日-2019 年 09 月 29 日 **2019 年第 39 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 505 个，其中高危漏洞 126 个、中危漏洞 327 个、低危漏洞 52 个。漏洞平均分值为 5.62。本周收录的漏洞中，涉及 0day 漏洞 171 个（占 34%），其中互联网上出现“YzmCMS 跨站请求伪造漏洞（CNVD-2019-33085）、WordPress yawpp 插件跨站脚本漏洞”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 3148 个，与上周（2794 个）环比增长 13%。

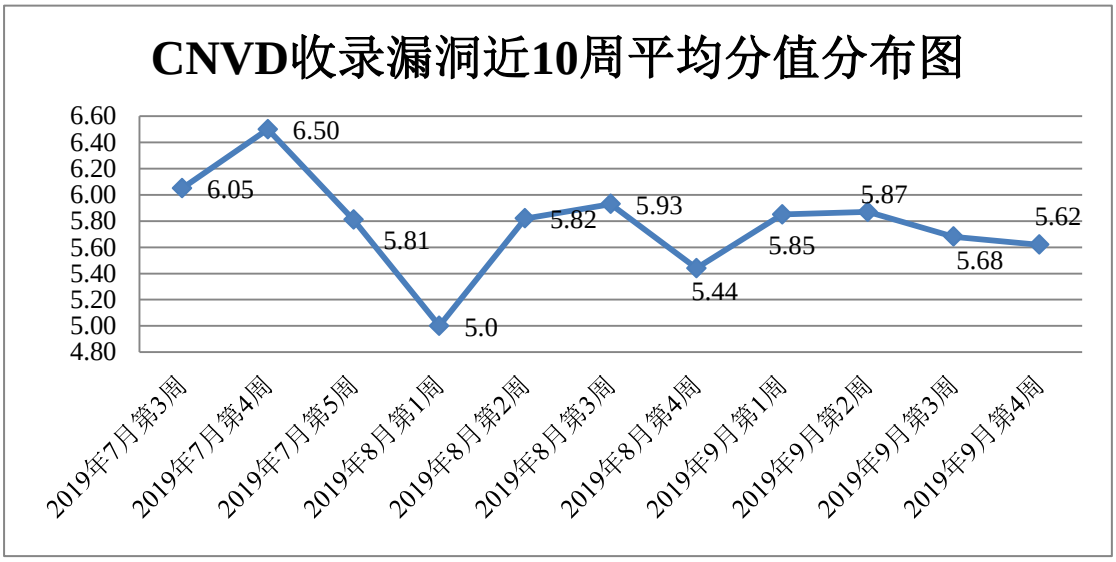

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 39 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 475 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 64 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30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：

北京易车信息科技有限公司、有品信息科技有限公司、苏州恩斯特网络科技有限公司、金蝶软件（中国）有限公司、中国中信股份有限公司、中国铁建重工集团股份有限公司、中国投融资担保股份有限公司、国旅投资发展有限公司、北京网御星云信息技术有限公司、中山市凝聚网络科技有限公司、淄博闪灵网络科技有限公司、上海企炬广告传媒有限公司、中国市政工程西南设计研究总院有限公司、深圳市天地心网络技术有限公司、南京路特软件有限公司、星网锐捷网络技术有限公司、广州恒企教育科技有限公司、北京东云创达科技有限公司、上海亿速网络科技有限公司、山西先启科技有限公司、北京良精志诚科技有限责任公司、成都火狐狸科技有限公司、上海鹏达计算机系统开发有限公司、杭州海康威视数字技术股份有限公司、鞍山中域网络科技有限公司、深圳市爱德数智科技股份有限公司、微点佰慧（北京）信息安全技术有限公司、广州热点软件科技股份有限公司、杭州当贝网络科技有限公司、灵吉网络科技有限公司、青岛易软天创网络科技有限公司、烟台云脉网络科技有限公司、北京广联达梦龙软件有限公司、深圳搜豹网络有限公司、微点佰慧(北京)信息安全技术有限公司、珠海金山办公软件有限公司、中国普联技术有限公司、北京博乐虎科技有限公司、广州市卓越里程教育科技有限公司、北京网康科技有限公司、普联技术有限公司、江苏汇文软件有限公司、奕司（上海）信息科技有限公司、原生态购物网、中国国际贸易促进委员会/中国国际商会调解中心、中环工作室、安徽启明星工作室、为因软件、睿谷信息科技、安优企业建站、中国国际社会公共安全产品博览会、DocCms X 开发团队、FineCMS、Adobe、ZZCMS、Zzzcms、Chinese Economist Society 和 Guojiz。

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。远江盛邦（北京）网络安全科技股份有限公司、长春嘉诚信息技术股份有限公司、南京众智维信息科技有限公司、山东新潮信息技术有限公司、北京铭图天成信息技术有限公司、国瑞数码零点实验室、山东云天安全技术有限公司、北京君信安科技有限公司、广州锦行网络科技有限公司、北京圣博润高新技术股份有限公司、山东华鲁科技发展股份有限公司、北京智游网安科技有限公司、上海市信息安全测评认证中心、上海银基信息安全技术股份有限公司、河南信安世纪科技有限公司及其他个人白帽子向 CNVD 提交了 3148 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 2284 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）	1285	1285
斗象科技（漏洞盒子）	993	993
北京天融信网络安全技术有限公司	305	1
哈尔滨安天科技集团股份有限公司	246	0
华为技术有限公司	143	0
四川无声信息技术有限公司	106	106
深信服科技股份有限公司	82	0
恒安嘉新(北京)科技股份公司	66	0
北京神州绿盟科技有限公司	57	0
厦门服云信息科技有限公司	56	1
新华三技术有限公司	55	0
北京启明星辰信息安全技术有限公司	43	1
浙江大华技术股份有限公司	14	14
北京数字观星科技有限公司	13	0
南京联成科技发展股份有限公司	10	10
沈阳东软系统集成工程有限公司	9	9
北京知道创宇信息技术股份有限公司	6	1
上海交大	6	6
西安四叶草信息技术有限公司	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	118	118
长春嘉诚信息技术股份有限公司	90	90
南京众智维信息科技有限公司	71	71
山东新潮信息技术有限公司	41	41
北京铭图天成信息技术有限公司	34	34
国瑞数码零点实验室	32	32
山东云天安全技术有限公司	25	25
北京君信安科技有限公司	14	14
广州锦行网络科技有限公司	14	14
北京圣博润高新技术股份有限公司	8	8
山东华鲁科技发展股份有限公司	7	7
北京智游网安科技有限公司	2	2
上海市信息安全测评认证中心	2	2
上海银基信息安全技术股份有限公司	2	2
河南信安世纪科技有限公司	1	1
河北分中心	15	15
宁夏分中心	10	10
浙江分中心	5	5
黑龙江分中心	2	2
个人	225	225
报送总计	4216	3148

本周漏洞按类型和厂商统计

本周，CNVD 收录了 505 个漏洞。应用程序 267 个，WEB 应用 168 个，网络设备（交换机、路由器等网络端设备）36 个，操作系统 25 个，数据库 5 个，安全产品 4 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	267
WEB 应用	168
网络设备（交换机、路由器等网络端设备）	36
操作系统	25
数据库	5
安全产品	4

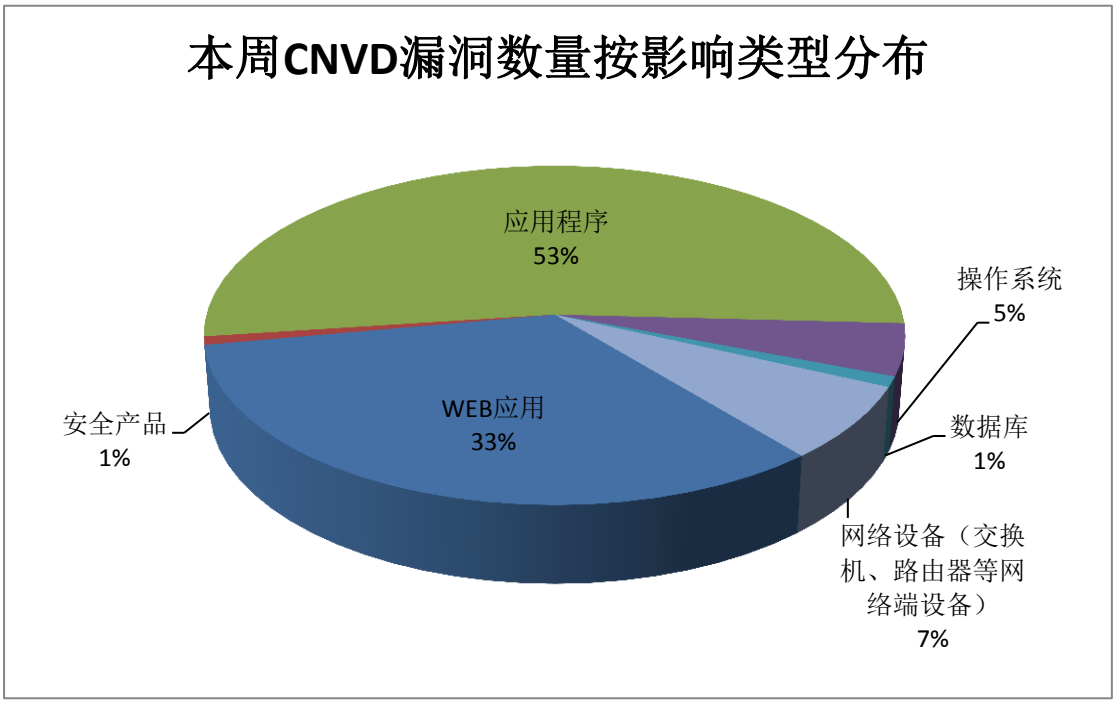

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Huawei、IBM 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	83	16%
2	Huawei	27	5%
3	IBM	26	5%
4	Apache	24	5%
5	Microsoft	22	4%
6	SAP	20	4%

7	ImageMagick Studio LLC	17	3%
8	GitLab	15	3%
9	Micro Focus	15	3%
10	其他	256	51%

本周行业漏洞收录情况

本周，CNVD 收录了 6 个电信行业漏洞，14 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“多款 Apple 产品 Kernel 组件资源管理错误漏洞、Symantec Norton Password Manager for Android 信息泄露漏洞”等漏洞的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/

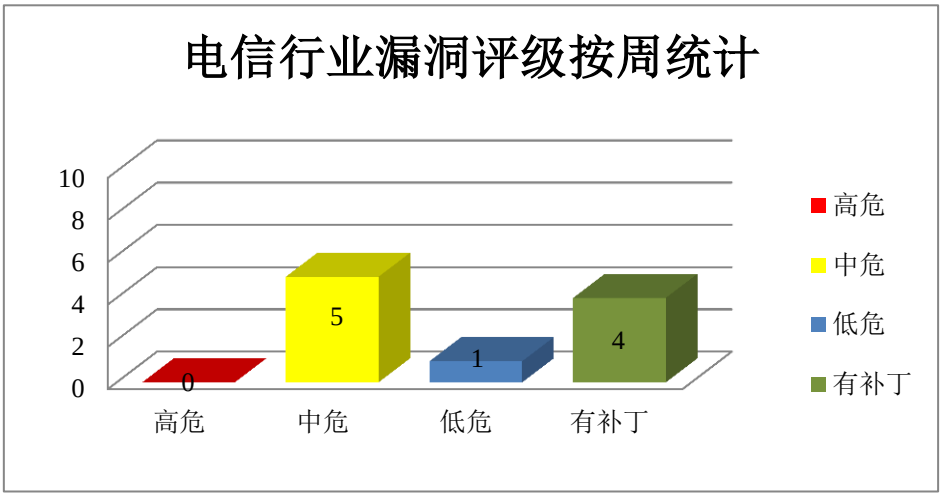

图 3 电信行业漏洞统计

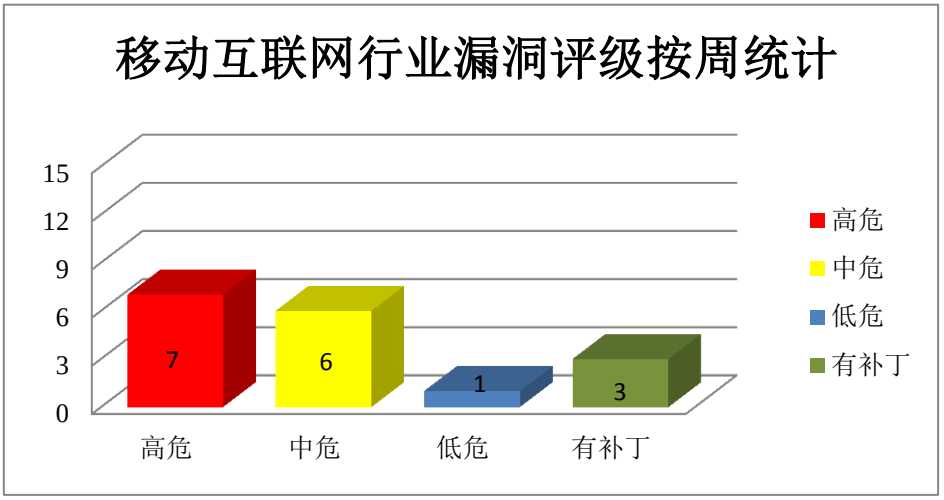

图 4 移动互联网行业漏洞统计

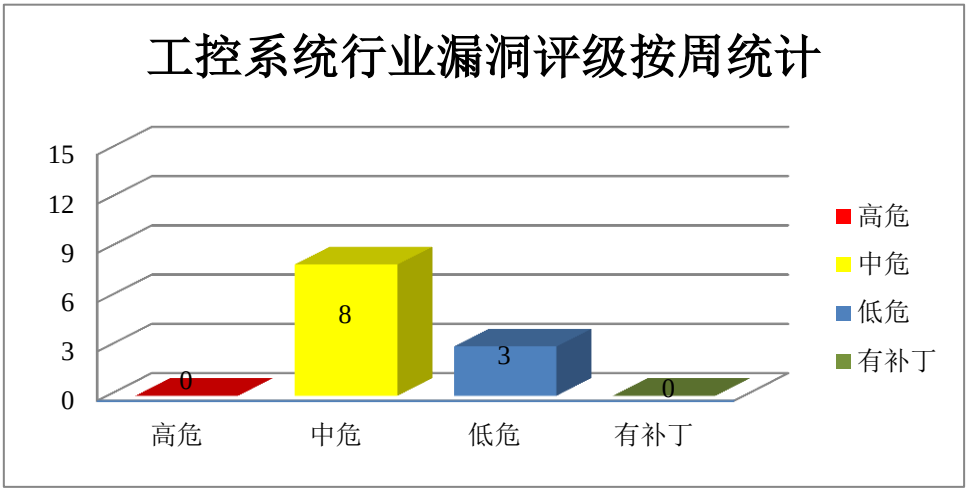

图 5 工控系统行业漏洞统计

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、Huawei 产品安全漏洞

Huawei P30 是一款智能手机。Huawei Mate RS 是一款智能手机。Huawei PCManager 是一套电脑管理软件。Huawei CloudEngine 6800 是一款面对数据中心的 6800 系列万兆以太网交换机。Huawei Emily-L29C 是一款智能手机。Huawei P20 是一款智能手机。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过 FRP 功能并获取权限，导致程序崩溃或执行任意代码等。

CNVD 收录的相关漏洞包括：Huawei P30 整形溢出漏洞（CNVD-2019-33477、CNVD-2019-33478）、Huawei Mate RS 锁屏绕过漏洞、Huawei PCManager 代码执行漏洞、Huawei CloudEngine 6800 鉴权不当漏洞、Huawei Emily-L29C 重释放漏洞、Huawei P20 FRP 安全绕过漏洞、Huawei Emily-L29C FRP 绕过漏洞。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-2019-33477

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33478

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33606

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33610

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33612

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33616

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33618

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33622

2、Microsoft 产品安全漏洞

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 Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。本周，上述产品被披露存在提权和远程代码执行漏洞，攻击者可利用漏洞提升权限，执行任意代码，造成内存破坏。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 远程代码执行漏洞、Microsoft Windows kernel image 提权漏洞、Microsoft Windows 和 Windows Server 提权漏洞（CNVD-2019-33312、CNVD-2019-33319、CNVD-2019-33320）、Microsoft Windows Kernel 提权漏洞（CNVD-2019-33327）、Microsoft DirectX 提权漏洞、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2019-33597）。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-2019-33310
http://www.cnvd.org.cn/flaw/show/CNVD-2019-33311
http://www.cnvd.org.cn/flaw/show/CNVD-2019-33312
http://www.cnvd.org.cn/flaw/show/CNVD-2019-33319
http://www.cnvd.org.cn/flaw/show/CNVD-2019-33320
http://www.cnvd.org.cn/flaw/show/CNVD-2019-33327
http://www.cnvd.org.cn/flaw/show/CNVD-2019-33325
http://www.cnvd.org.cn/flaw/show/CNVD-2019-33597

3、Apache 产品安全漏洞

Apache Tapestry 是一款使用 Java 语言编写的 Web 应用程序框架。Apache OFBiz 是一套企业资源计划（ERP）系统。Apache Commons Compress 是一个用于处理压缩文件的库。Apache VCL 是一套开源的云计算平台。Apache httpd 是一款专为现代操作系统开发和维护的开源 HTTP 服务器。Apache PDFBox 是一款基于 Java 语言的开源工具库。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，造成拒绝服务（崩溃）等。

CNVD 收录的相关漏洞包括：Apache Tapestry 代码问题漏洞、Apache OFBiz 代码执行漏洞、Apache OFBiz java.io.ObjectInputStream 反序列化代码执行漏洞、Apache httpd mod_http2 拒绝服务漏洞、Apache Commons Compress 拒绝服务漏洞、Apache VCL 输入验证错误漏洞、Apache httpd 缓冲区溢出漏洞（CNVD-2019-33835）、Apache PDFBox 代码问题漏洞。其中，除“Apache Commons Compress 拒绝服务漏洞、Apache httpd 缓冲区溢出漏洞（CNVD-2019-33835）”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-2019-33625

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33825

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33827

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33830

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33833

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33837

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33835

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33839

4、IBM 产品安全漏洞

IBM Security Key Lifecycle Manager（Tivoli Key Lifecycle Manager）是一套密钥生命周期管理软件。IBM DB2 是一套关系型数据库管理系统。IBM Cognos Analytics 一套商业智能软件。IBM API Connect（APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM Cognos Analytics 是一套商业智能软件。IBM Spectrum Protect Plus 是一套数据保护平台。IBM MQ（IBM WebSphere MQ）是一款消息传递中间件产品。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，执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Security Key Lifecycle Manager 信息泄露漏洞（NVD-C-2019-137712）、IBM DB2 缓冲区溢出漏洞（CNVD-2019-33768）、IBM Cognos Analytics 拒绝服务漏洞、IBM DB2 High Performance Unload load for LUW 权限许可和访问控制问题漏洞、IBM API Connect 访问控制错误漏洞、IBM Cognos Analytics 路径遍历漏洞、IBM Spectrum Protect Plus 权限许可和访问控制问题漏洞（CNVD-2019-33776）、IBM MQ 权限许可和访问控制问题漏洞。其中，除“IBM Security Key Lifecycle Manager 信息泄露漏洞（NVD-C-2019-137712）、IBM Cognos Analytics 路径遍历漏洞”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-2019-33294

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33768

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33765

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33774

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33778

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33779

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33776

http://www.cnvd.org.cn/flaw/show/CNVD-2019-33782

5、LG GAMP-7100、GAPM-7200 和 GAPM-8000 信息泄露漏洞

LG GAMP-7100 等都是韩国乐金（LG）公司的一款路由器。本周，LG GAMP-7100、GAPM-7200 和 GAPM-8000 被披露存在信息泄露漏洞。未授权的攻击者可利用漏洞

获取受影响组件敏感信息。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-2019-33821

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-2019-33594	FreeBSD 内核内存泄露漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.freebsd.org/pipermail/freebsd-announce/2019-August/001909.html
CNVD-2019-33599	SamsungTTS 组件权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.smartthings.com/
CNVD-2019-33624	Huawei Hima-AL00B 内存重释放漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20190220-01-smartphone-cn
CNVD-2019-33626	EXIM4 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://exim.org
CNVD-2019-33712	Foxit Studio Photo 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://www.foxitsoftware.com/downloads/#Foxit-Studio-Photo/
CNVD-2019-33738	ImageMagick Studio ImageMagick 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/ImageMagick/ImageMagick/issues/1221
CNVD-2019-33758	WordPress Tevolution 插件代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://templatic.com/wordpress-plugins/tevolution/
CNVD-2019-33802	Yandex ClickHouse 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://clickhouse.yandex/docs/en/security_changelog/
CNVD-2019-33822	Cisco Small Business RV320 和 RV325 授权问题漏洞	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/c

			ontent/CiscoSecurityAdvisory/cisco-sa-20190501-sbr-hijack
CNVD-2019-33851	Google Chrome V8 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop.html

小结：本周，Huawei 产品被披露存在多个漏洞，攻击者可利用漏洞绕过 FRP 功能并获取权限，导致程序崩溃或执行任意代码等。此外，Microsoft、Apache、IBM 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，提升权限，执行任意代码，造成拒绝服务等。另外，LG GAMP-7100、GAPM-7200 和 GAPM-8000 被披露存在信息泄露漏洞。未授权的攻击者可利用漏洞获取受影响组件敏感信息。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 yawpp 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。yawpp 是使用在其中的一个网上请愿插件。

WordPress yawpp 插件 1.2.2 及之前版本中存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：http://www.iwantacve.cn/index.php/archives/31

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-33103

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. 微软 Internet Explorer 浏览器 Jscript.Dll 组件远程代码执行漏洞

近日，微软发布了针对 Internet Explorer 浏览器组件 jscript.dll 的漏洞修复补丁，

该漏洞由 Google 威胁分析小组的安全研究员 ClémentLecigne 发现，成功利用此漏洞会破坏内存，使攻击者能够执行任意代码，攻击者可能会利用这个漏洞通过挂马网站的形式传播恶意代码。

参考链接：https://www.freebuf.com/vuls/215436.html

2. 不可修补的 iOS 漏洞可能导致 iPhone 4s 到 iPhone X 永久越狱

一名安全研究人员发布了据称是 iPhone 4s 直至 iPhone X 永久性，不可修补的 boo trom 漏洞，这可能导致永久越狱。Twitter 用户 axi0mX 今天分享了这个漏洞，并且命名为“ checkm8”，如果该漏洞进一步加以利用，将导致史诗般的越狱。

参考链接：https://www.cnbeta.com/articles/tech/894205.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