国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 10 月 21 日-2019 年 10 月 27 日 **2019 年第 43 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 479 个，其中高危漏洞 125 个、中危漏洞 324 个、低危漏洞 30 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 106 个（占 22%），其中互联网上出现“D-Link DIR-816 输入验证错误漏洞、Kirona Solutions Dynamic Resource Scheduling 信息泄露漏洞”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 9602 个，与上周（3527 个）环比增长 1.72 倍。

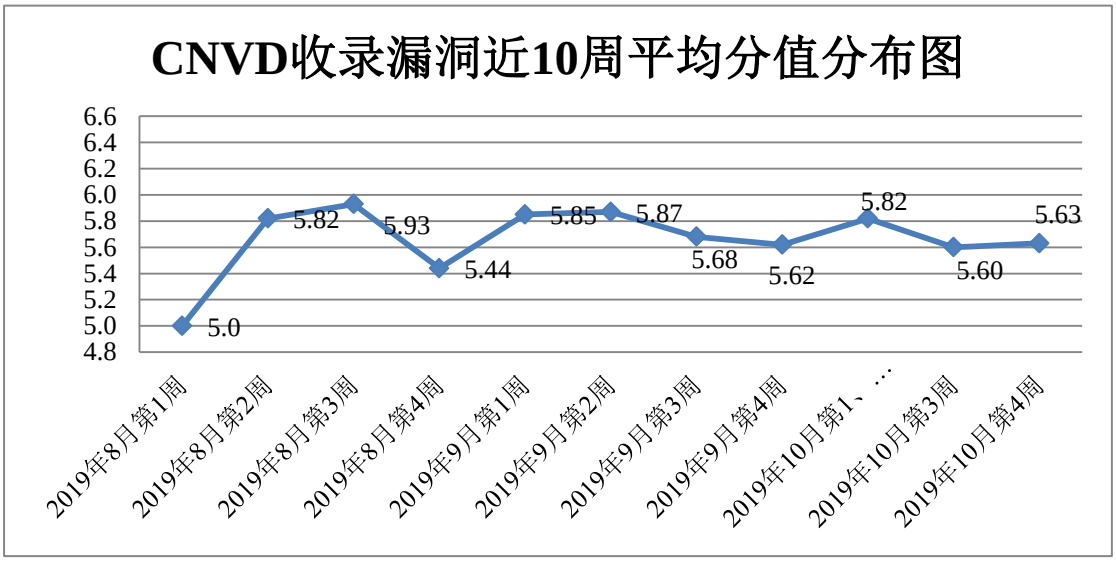

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 1 起，向银行、保险、能源等重要行业单位通报漏洞事件 22 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 719 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 107 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22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：

西安佰联网络技术有限公司、深圳市龙艺脉网络科技有限公司、帝兴软件开发有限公司、中国化学工程第十三建设有限公司、洪湖尔创网联信息技术有限公司、捷豹路虎（中国）投资有限公司、武汉创益云信息技术有限公司、苏州托普斯网络科技有限公司、北京对啊网教育科技有限公司、北京良精志诚科技有限责任公司、南京酷奇信息科技有限公司、青岛拓宇网络科技有限公司、武汉京伦科技有限公司、云研网络科技有限公司、嘉兴想天信息科技有限公司、中国检验认证集团山西有限公司、昆明云涛科技有限公司、中国检验认证集团广东有限公司、湖北源尖软件科技有限公司、广州拓波软件科技有限公司、岳阳易发网络科技有限公司、哈尔滨伟成科技有限公司、深圳市惠尔顿信息技术有限公司、上海泛微网络科技股份有限公司、洛阳市万谦网络科技有限公司、中控智慧科技股份有限公司、上海晓材科技有限公司、中国灵吉网络科技公司、北京永信至诚科技股份有限公司、深一科技集团有限公司、成都爱米秀科技有限责任公司、深圳市爱思软件技术有限公司、淄博闪灵网络科技有限公司、中粮集团有限公司、中铁一局集团有限公司、北京心海导航科技有限公司、湖南翱云网络科技有限公司、太原迅易科技有限公司、国药集团动物保健股份有限公司、苏州塔尖信息科技有限公司、法治中国普法教育工作办公室、中国铁道工程建设协会、安徽启明星工作室、中国招标采购培训网、国家油气田井口设备质量监督检验中心、中国电子政务网、一鸣网络、梦雨 cms、易优CMS、Guojiz、SchoolCMS、ZhiCms、KiteCMS、Pluck CMS、UQCMS、Kkcms、UCMS、SemCms、Zzzcms、OurHouse 和 Gxlcms。

本周，CNVD 发布了《Oracle 发布 2019 年 10 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5255

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、北京神州绿盟科技有限公司、厦门服云信息科技有限公司、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、长春嘉诚信息技术股份有限公司、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、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、广州锦行网络科技有限公司、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、北京君信安科技有限公司、内蒙古奥创科技有限公司、任子行网络技术股份有限公司、北京智游网安科技有限公司、北京容辉智

信科技有限公司、北京圣博润高新技术股份有限公司、河南信安世纪科技有限公司、上海端御信息科技有限公司、重庆贝特计算机系统工程有限公司、腾讯公司、山石网科通信技术股份有限公司、深圳市魔方安全科技有限公司、新疆海狼科技有限公司及其他个人白帽子向 CNVD 提交了 9602 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 8704 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）	6437	6437
斗象科技（漏洞盒子）	1850	1850
上海交大	417	417
北京天融信网络安全技术有限公司	307	10
哈尔滨安天科技集团股份有限公司	252	0
北京神州绿盟科技有限公司	192	0
厦门服云信息科技有限公司	124	0
深信服科技股份有限公司	119	1
华为技术有限公司	95	0
恒安嘉新(北京)科技股份公司	74	0
北京启明星辰信息安全技术有限公司	53	0
西安四叶草信息技术有限公司	21	21
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	19	19
阿里云计算有限公司	18	0
新华三技术有限公司	15	0
中国电信集团系统集成有限责任公司	14	14

南京联成科技发展股份有限公司	3	3
北京知道创宇信息技术股份有限公司	2	0
远江盛邦（北京）网络安全科技股份有限公司	136	136
国瑞数码零点实验室	97	97
长春嘉诚信息技术股份有限公司	91	91
山东新潮信息技术有限公司	49	49
北京铭图天成信息技术有限公司	34	34
山东云天安全技术有限公司	29	29
南京众智维信息科技有限公司	26	26
广州锦行网络科技有限公司	24	24
杭州海康威视数字技术股份有限公司	15	15
北京华云安信息技术有限公司	13	13
北京君信安科技有限公司	8	8
内蒙古奥创科技有限公司	7	7
任子行网络技术股份有限公司	5	5
北京智游网安科技有限公司	3	3
北京容辉智信科技有限公司	2	2
北京圣博润高新技术股份有限公司	2	2
河南信安世纪科技有限公司	2	2
上海端御信息科技有限公司	2	2
重庆贝特计算机系统工程有限公司	2	2
腾讯公司	1	1

山石网科通信技术股份有限公司	1	1
深圳市魔方安全科技有限公司	1	1
新疆海狼科技有限公司	1	1
个人	279	279
报送总计	10862	9602

本周漏洞按类型和厂商统计

本周，CNVD 收录了 479 个漏洞。应用程序 245 个，操作系统 99 个，WEB 应用 47 个，数据库 37 个，网络设备（交换机、路由器等网络端设备）34 个，智能设备（物联网终端设备）漏洞 12 个，安全产品 5 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	245
操作系统	99
WEB 应用	47
数据库	37
网络设备（交换机、路由器等网络端设备）	34
智能设备（物联网终端设备）漏洞	12
安全产品	5

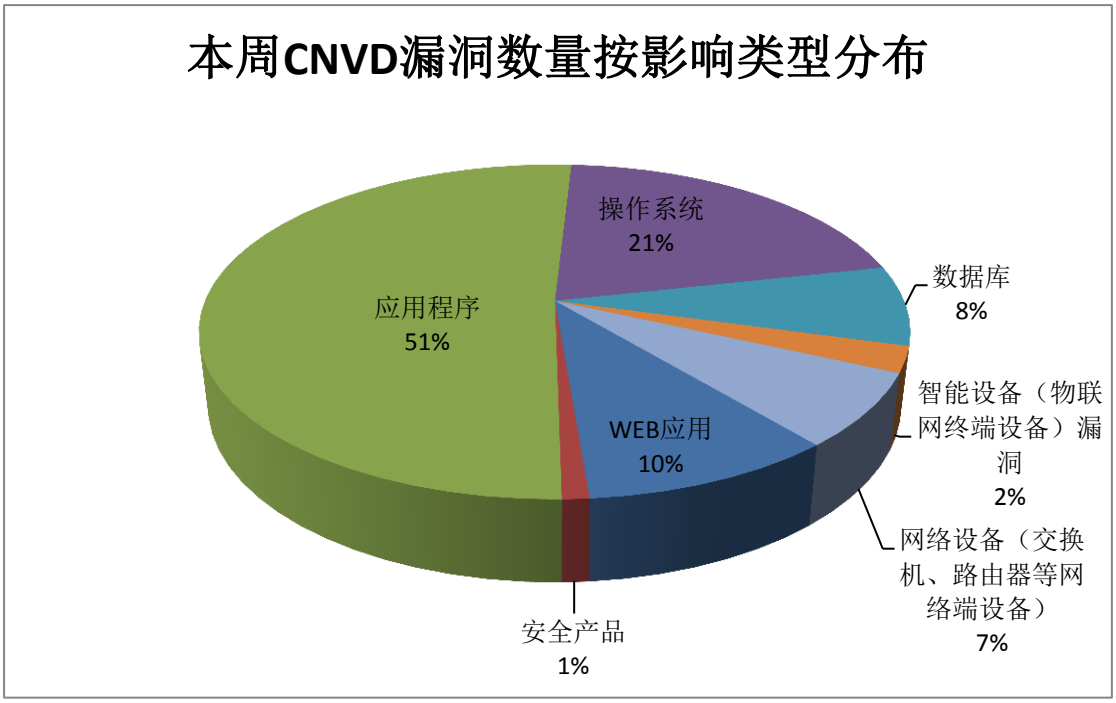

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、Cisco 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	87	18%
2	Google	59	12%
3	Cisco	46	10%
4	Apple	35	7%
5	Microsoft	14	3%
6	Adobe	13	3%
7	FasterXML	10	2%
8	MediaWiki	10	2%
9	Palo Alto Networks	10	2%
10	其他	195	41%

本周行业漏洞收录情况

本周，CNVD 收录了 27 个电信行业漏洞，84 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Apple iTunes 和 iCloud for Windows 内存破坏漏洞、IEC870IP driver 缓冲区溢出漏洞、Google Android MNH 提权漏洞（CNVD-2019-36641）、NETGEAR JNR1010 访问控制错误漏洞、Cisco IOS XE FTP ALG 拒绝服务漏洞”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/

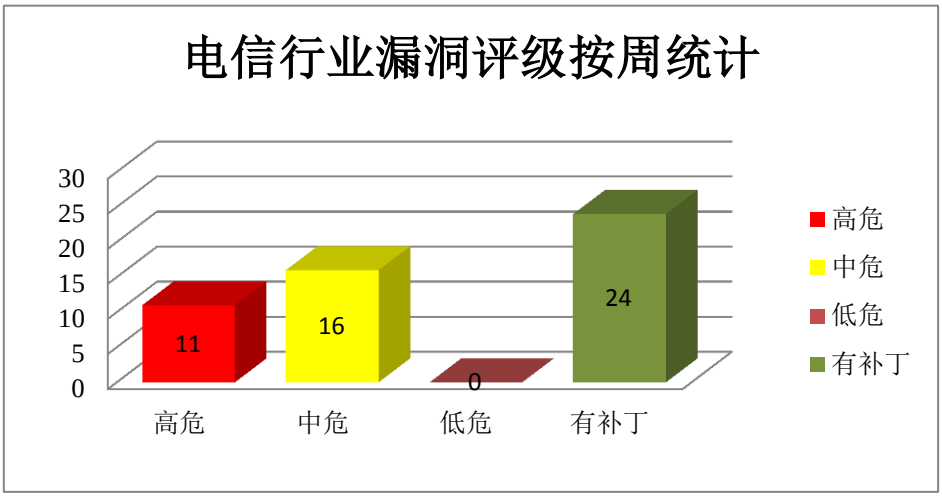

图 3 电信行业漏洞统计

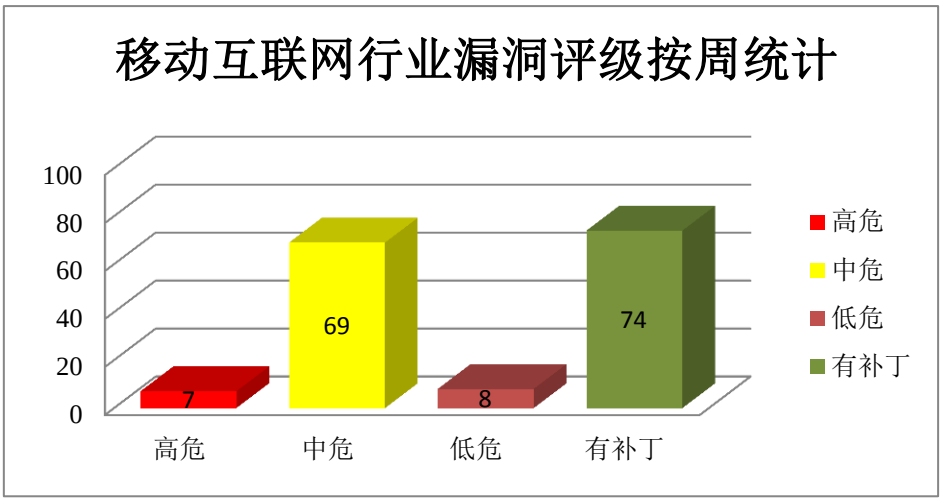

图 4 移动互联网行业漏洞统计

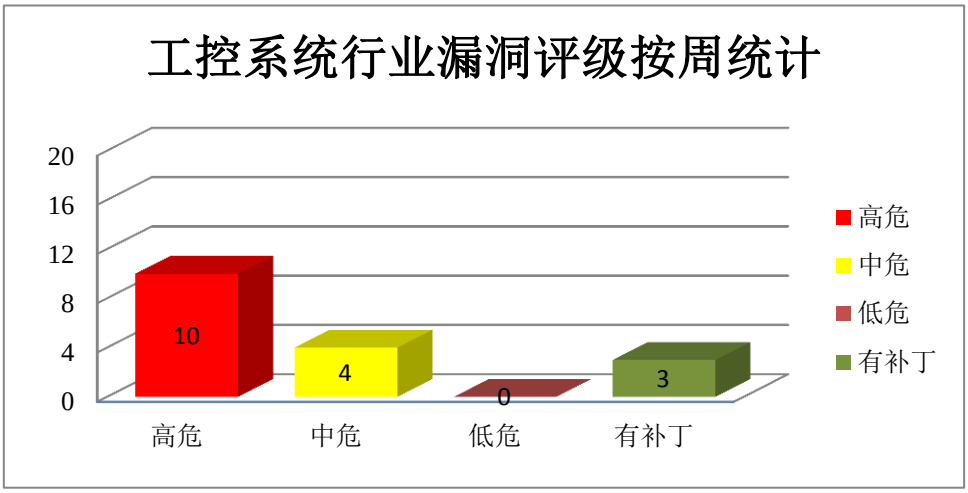

图 5 工控系统行业漏洞统计

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 是一款 Web 浏览器。Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 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，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码或造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2019-36440）、Google Android MNH 提权漏洞（CNVD-2019-36641）、Google Chrome audio 资源管理错误漏洞、Google Chrome V8 资源管理错误漏洞（CNVD-2019-36924）、Google Chrome IndexedDB 资源管理错误漏洞、Google Chrome WebRTC 资源管理错误漏洞、Google Android 拒绝服务漏洞（CNVD-2019-37159、CNVD-2019-37160）。其中，除“Google Android 信息泄露漏洞（CNVD-2019-36440）、Google Android 拒绝服务漏洞（CNVD-2019-37159、CNVD-2019-37160）”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-2019-36440

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36641

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36905

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36924

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36945

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36948

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37159

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37160

2、Cisco 产品安全漏洞

Cisco Wireless LAN Controller（WLC）Software 是一套用于配置和管理 WLC（无线局域网控制器）的软件。Cisco IOS XE 是为其网络设备开发的一套基于 Linux 内核的模块化操作系统。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命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Wireless LAN Controller Software 输入验证错误漏洞、Cisco IOS XE 虚拟化管理器 CLI 命令注入漏洞、Cisco IOS XE UTD 拒绝服务漏洞、Cisco IOS XE 拒绝服务漏洞（CNVD-2019-36642）、Cisco IOS XE NAT SIP ALG 拒绝服务漏洞、Cisco IOS XE FTP ALG 拒绝服务漏洞、Cisco IOS XE CTS PAC 配置拒绝服务漏洞、Cisco IOS XE 任意代码执行漏洞。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-2019-36455

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36644

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36645

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36642

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36643

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36646

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36652

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36655

3、Apple 产品安全漏洞

Apple macOS Catalina 是一套专为 Mac 计算机所开发的专用操作系统。Apple iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。Apple iCloud for Windows 是一款基于 Windows 平台的云服务，它支持存储音乐、照片、App 和联系人等。Apple Xcode 是一套向开发人员提供的集成开发环境，它主要用于开发 Mac OS X 和 iOS 的应用程序。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：Apple macOS Catalina Intel Graphics Driver 组件内存破坏漏洞、Apple macOS Catalina AMD 组件内存破坏漏洞、Apple macOS Catalina sips 组件内存破坏漏洞、Apple iTunes 和 iCloud for Windows 内存破坏漏洞、Apple macOS Catalina 内存破坏漏洞、Apple Xcode otool 组件任意代码执行漏洞（CNVD-2019-37180）、Apple Xcode ld64 组件任意代码执行漏洞（CNVD-2019-37184、CNVD-2019-37185）。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-2019-36605

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36607

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36608

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36610

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36614

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37180

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37184

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37185

4、Microsoft 产品安全漏洞

Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码，从而可获得与当前用户相同的用户权限。

CNVD 收录的相关漏洞包括：Microsoft Edge Chakra 脚本引擎内存破坏漏洞（CNVD-2019-36634、CNVD-2019-36635、CNVD-2019-36637、CNVD-2019-36636、CNVD-2019-36876、CNVD-2019-36877、CNVD-2019-36878、CNVD-2019-36879）。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-2019-36634

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36635

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36637

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36636

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36876

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36877

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36878

http://www.cnvd.org.cn/flaw/show/CNVD-2019-36879

5、MATIO 'Mat_VarReadNextInfo4'函数缓冲区溢出漏洞

MATIO 是一款用于读写二进制 MATLAB MAT 文件的开源 C 语言库。本周，MAT IO 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-2019-36862

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-2019-36471	NETGEAR JNR1010 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.netgear.com/30177/JNR1010-Firmware-Version-1-0-0-32
CNVD-2019-36671	Palo Alto Networks Zingbox Inspector 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://securityadvisories.paloaltonetworks.com/Home/Detail/167
CNVD-2019-36973	idreamsoft iCMS spider_project.admincp.php 文件 SQL 注入漏洞	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/idreamsoft/iCMS
CNVD-2019-36979	CloudCTI HIP Integrator Recognition Configuration Tool 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.cloudcti.nl/
CNVD-2019-36986	AutoPi.io AutoPi Wi-Fi/NB 和 AutoPi 4G/LTE 暴力攻击漏洞	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.autopi.io
CNVD-2019-36992	QEMU 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://github.com/qemu/qemu/commit/659142ecf71a0da240ab0ff7cf929ee25c32b9bc
CNVD-2019-36994	NVIDIA Shield TV Experience 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://nvidia.custhelp.com/app/answers/detail/a_id/4875
CNVD-2019-37153	FasterXML jackson-databind 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://github.com/FasterXML/jackson-databind/compare/jackson-databind-2.9.9.1...jackson-databind-2.9.9.2
CNVD-2019-36855	PHP 远程代码执行漏洞（CNVD-2019-36855）	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://bugs.php.net/bug.php?id=78599
CNVD-2019-36982	Sudo 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.sudo.ws/alerts/minus_1_uid.html

小结：本周，Google 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，执行任意代码或造成拒绝服务。此外，Cisco、Apple、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命令，导致拒绝服务等。另外，MATIO 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、D-Link DIR-816 输入验证错误漏洞

验证描述

D-Link DIR-816 是中国台湾友讯（D-Link）公司的一款无线路由器。

D-Link DIR-816 A1 1.06 版本中存在安全漏洞。攻击者可利用该漏洞访问路由器的管理页面。

验证信息

POC 链接：https://github.com/dahua966/Routers-vuls/tree/master/DIR-816

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-36946

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. 黑客恶意利用 PHP7 远程执行代码漏洞

PHP7 中的一个远程代码执行漏洞（CVE-2019-11043）在野利用被发现。安全专家 Omar Ganiev 通过 Twitter 宣布了 PHP-FPM（PHP 的 FastCGI 流程管理器（FPM））中“新补丁”对于远程代码执行漏洞的有效性 。CVE-2019-11043 漏洞不需要使用特定技能即可接入服务器，它是 PHP-FPM 的 fpm_main.c 中的 env_path_info 下溢漏洞。这意味着该问题仅影响启用 PHP-FPM 的 NGINX 服务器。

参考链接：https://securityaffairs.co/wordpress/92997/hacking/cve-2019-11043-php7-flaw.html

2. 浏览器 Maxthon 中发现的恶意软件授予管理员权限的漏洞

根据网络安全公司 SafeBREACH 的一份报告，中国最受欢迎的网络浏览器 Maxthon 中存在一个易于利用的漏洞。该漏洞允许恶意软件在 Maxthon 的某个组件的帮助下获得管理员权限和引导持久性。SafeBREACH 研究人员在 9 月初向 Maxthon 开发人员报告了该漏洞，但该公司尚未发布更新。

参考链接：https://www.zdnet.com/article/bug-that-grants-admin-rights-to-malware-found-in-maxthon-chinas-favorite-browser/

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