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 02 日-2019 年 09 月 08 日　　2019 年第 36 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 709 个，其中高危漏洞 241 个、中危漏洞 413 个、低危漏洞 55 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 359 个（占 51%），其中互联网上出现“YouPHPTube 远程代码执行漏洞、ASUS SmartHome Gateway HG100 拒绝服务漏洞”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（2022 个）环比增长 55%。

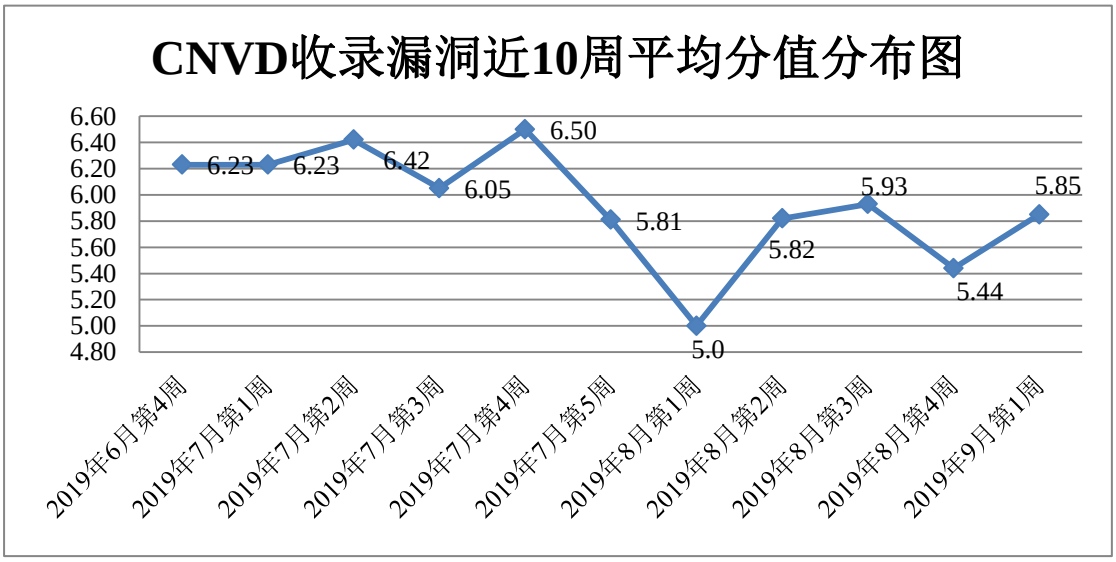

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 3 起，向银行、保险、能源等重要行业单位通报漏洞事件 12 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 407 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 102 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24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：

江苏楚淮软件科技开发有限公司、国药控股沈阳有限公司、河南网中网计算机科技有限公司、中国绿色建筑与节能专业委员会绿色校园学科组、北京通达信科科技有限公司、友讯电子设备（上海）有限公司、深圳市新普软件开发有限公司、上海卓越睿新数码科技有限公司、沧州市凡诺广告传媒有限公司、施耐德电气(中国)有限公司、青岛飞鸽软件有限公司、摩莎科技（上海）有限公司、桂林崇胜网络科技有限公司、广州聆科网络技术有限公司、北京壹零叁玖科技发展有限公司、成都康菲顿特网络科技有限公司、福建银达汇智信息科技股份有限公司、锐捷网络股份有限公司、沈阳河汉科技有限公司、沈阳盘古网络技术有限公司、上海复翼软件开发有限公司、灵宝简好网络科技有限公司、淄博闪灵网络科技有限公司、北京豪纳睿斯科技有限公司、深圳市懒人在线科技有限公司、广东亦强科技有限公司、中农万嘉鲜实业发展股份有限公司、成都卓越远扬信息技术有限公司、石家庄灵石科技有限公司、中国十九冶集团有限公司、嘉兴想天信息科技有限公司、深圳市锟锆科技有限公司、中国船舶重工集团柴油机有限公司、广州恒企教育科技有限公司、汕头市三互科技有限公司、深圳搜豹网络有限公司、四川迅睿云软件开发有限公司、长沙友点软件科技有限公司、南大傲拓科技江苏有限公司、桂林快特网络科技有限公司、成都爱诚科技有限公司、厦门海为科技有限公司、河北康吉森自动化工程有限公司、深圳市动力启航软件有限公司、浙江搜派信息科技有限公司、桂林快特网络科技有限公司、SOFTONIC 国际公司、睿谷信息科技、北京市农林科学院农业信息与经济研究所、闻泰网络、特种装备网、中国 3.15 诚信建设联盟会员中心办公室、袁志蒙工作室、如斯团队、中国电子标准协会培训中心、华夏 ERP、DuomiCms、PHPMyWind、HadSky、Notepad++、Zebra、Phpmywind、MyBB Group 和 ShopXO。

本周，CNVD 发布了《关于 Microsoft 远程桌面服务存在远程代码执行漏洞的安全公告（第二版）》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5195

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、深信服科技股份有限公司、华为技术有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。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、远江盛邦（北京）网络安全科技股份有限公司、山东云天安全技术有限公司、任子行网络技术股份有限公司、国瑞数码零点实验室、南京众智维信息科技有限公司、北京君信安科技有限公司、山东新潮信息技术有限公司、山石网科通信技术股份有限公司、内蒙古奥创科技有限公司、北京智游网安科技有限公司、北京圣博润高新技术股份有限公司、开普云信息科技股份有限公司、山东华鲁科技发展股份有限公

司、上海市信息安全测评认证中心、深圳市魔方安全科技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2575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）	1203	1203
奇安信网神（补天平台）	1088	1088
北京天融信网络安全技术有限公司	380	6
上海交大	284	284
哈尔滨安天科技集团股份有限公司	208	0
深信服科技股份有限公司	118	0
华为技术有限公司	86	0
新华三技术有限公司	50	0
北京启明星辰信息安全技术有限公司	49	0
恒安嘉新(北京)科技股份公司	49	0
北京神州绿盟科技有限公司	35	0
北京数字观星科技有限公司	20	0
西安四叶草信息技术有限公司	8	8
北京知道创宇信息技术股份有限公司	3	1
沈阳东软系统集成工程有限公司	2	2
长春嘉诚信息技术股份有限公司	159	159
北京铭图天成信息技术有限公司	68	68
远江盛邦（北京）网络安全科技股份有限公司	51	51
山东云天安全技术有限公司	29	29

任子行网络技术股份有限公司	25	25
国瑞数码零点实验室	22	22
南京众智维信息科技有限公司	20	20
北京君信安科技有限公司	7	7
山东新潮信息技术有限公司	7	7
山石网科通信技术股份有限公司	4	4
内蒙古奥创科技有限公司	3	3
北京智游网安科技有限公司	2	2
北京圣博润高新技术股份有限公司	2	2
开普云信息科技股份有限公司	1	1
山东华鲁科技发展股份有限公司	1	1
上海市信息安全测评认证中心	1	1
深圳市魔方安全科技有限公司	1	1
CNCERT 西藏分中心	15	15
CNCERT 贵州分中心	3	3
CNCERT 吉林分中心	2	2
CNCERT 山西分中心	1	1
个人	124	124
报送总计	4131	3140

本周漏洞按类型和厂商统计

本周，CNVD 收录了 709 个漏洞。WEB 应用 373 个，应用程序 268 个，操作系统 39 个，网络设备（交换机、路由器等网络端设备）20 个，智能设备（物联网终端设备）漏洞 5 个，安全产品 3 个，数据库 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
WEB 应用	373
应用程序	268
操作系统	39
网络设备（交换机、路由器等网络端设备）	20
智能设备（物联网终端设备）漏洞	5
安全产品	3
数据库	1

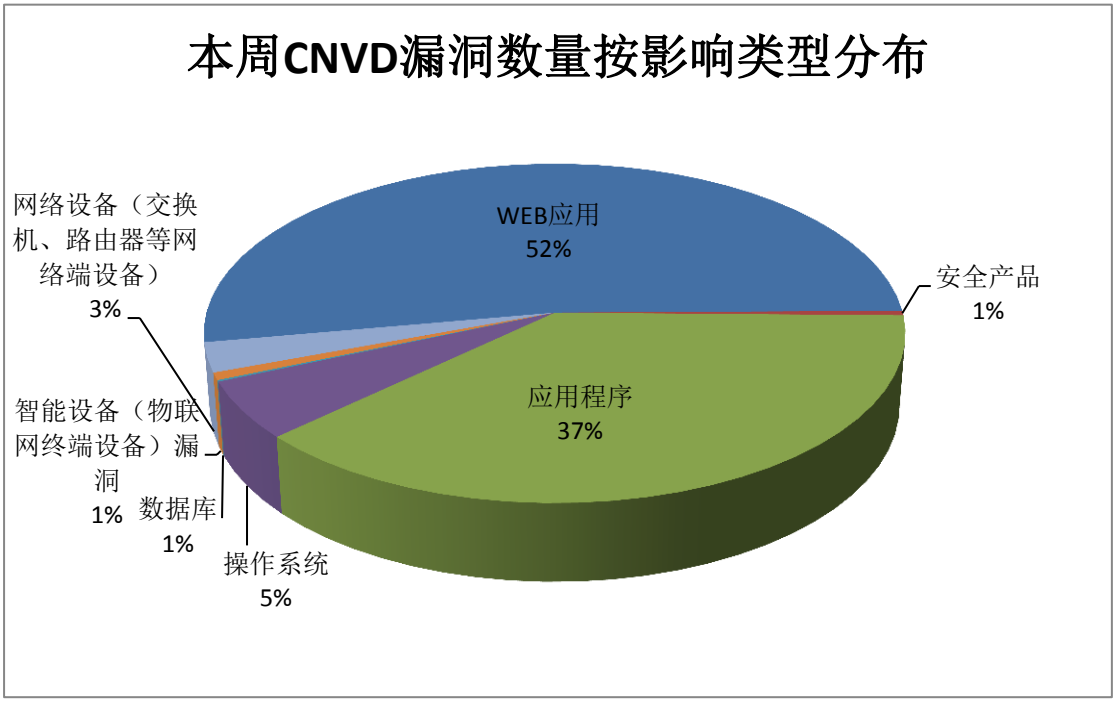

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Google、CloudBees 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	164	23%
2	Google	37	5%
3	CloudBees	23	3%
4	cPanel	23	3%
5	GitLab	11	2%
6	Adobe	19	3%
7	Odoo	14	2%

8	ACD Systems International	13	2%
9	Mozilla	12	2%
10	其他	393	55%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，58 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Google Android NVIDIA BootROM 提权漏洞、Google Android Media framework 远程代码执行漏洞（CNVD-2019-30325）、Google Android System 权限提升漏洞（CNVD-2019-30316）”等漏洞的综合评级为“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/

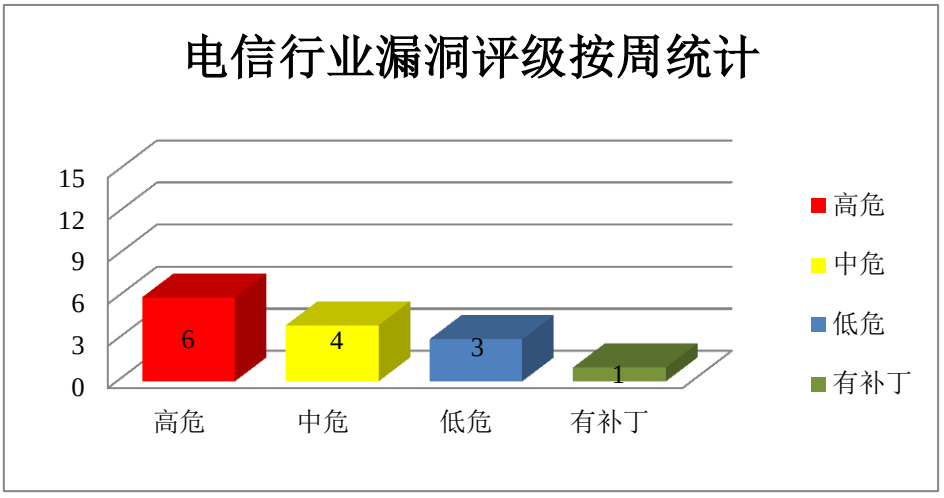

图 3 电信行业漏洞统计

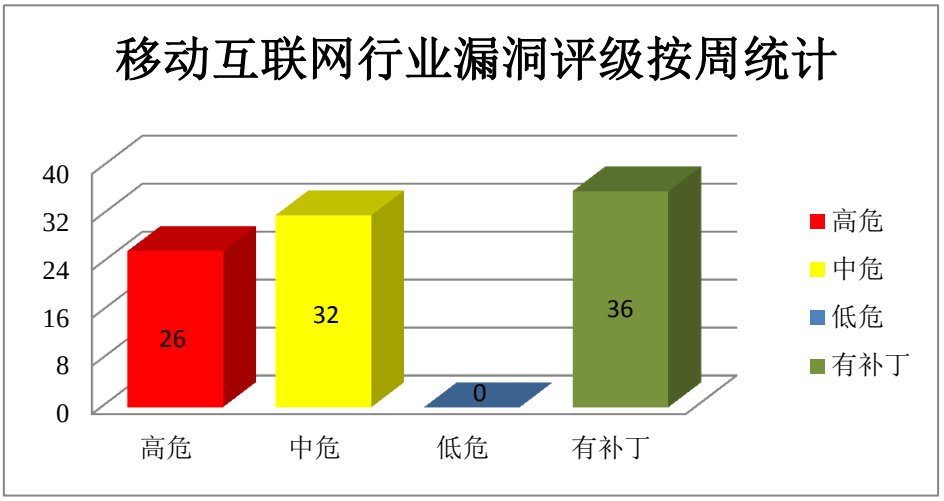

图 4 移动互联网行业漏洞统计

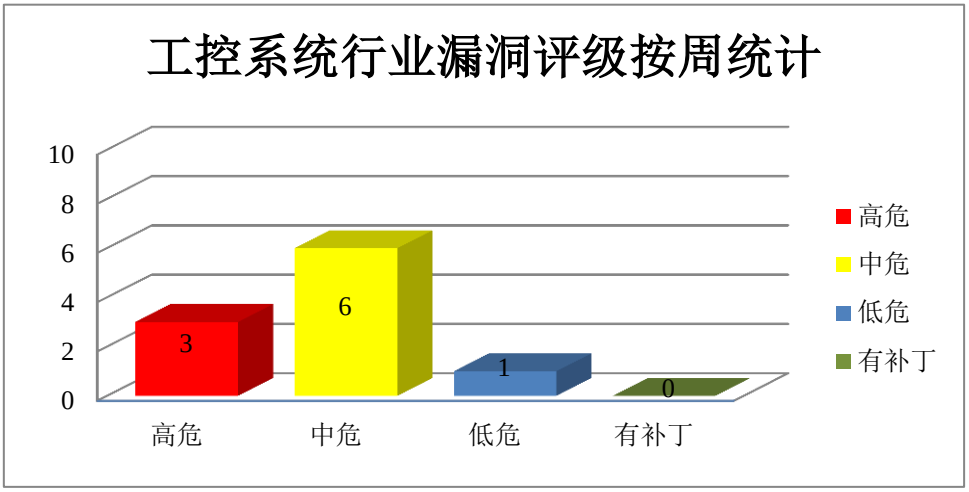

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

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，上述产品被披露存在信息泄露和远程代码执行漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Media framework 远程代码执行漏洞（CNVD-2019-30324、CNVD-2019-30325）、Google Android System 远程代码执行漏洞（CNVD-2019-30326）、Google Android Media Framework 信息泄露漏洞（CNVD-2019-30344、CNVD-2019-30346、CNVD-2019-30348、CNVD-2019-30368、CNVD-2019-30370）。其中，“Google Android Media framework 远程代码执行漏洞（CNVD-2019-30324、CNVD-2019-30325）、Google Android System 远程代码执行漏洞（CNVD-2019-30326）”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-2019-30324

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30325

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30326

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30344

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30346

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30348

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30368

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30370

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。Adobe Flash Player 是一种广泛使用的、专有的多媒体程序播放器，最初由 Macromedia 编写，在 Macromedia 被 Adobe 收购后由 Adobe 继续开发并分发。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。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 不可信指针解引用漏洞（CNVD-2019-30081、CNVD-2019-30091、CNVD-2019-30092）、Adobe Flash Player 内存错误引用漏洞（CNVD-2019-30084）、Adobe Acrobat/Reader 类型混淆漏洞（CNVD-2019-30082）、Adobe Acrobat/Reader 双重释放漏洞（CNVD-2019-30087）、Adobe Acrobat/Reader 命令注入漏洞、Adobe Acrobat/Reader 缓冲区溢出漏洞（CNVD-2019-30094）。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-2019-30081

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30084

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30082

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30087

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30091

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30093

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30094

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30092

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过同源策略并获取敏感信息，提升权限，执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2019-30437）、Mozilla Firefox 未授权访问漏洞（CNVD-2019-30438）、Mozilla Firefox 权限提升漏洞（CNVD-2019-30440）、Mozilla Firefox 资源管理错误漏洞（CNVD-2019-30439、CNVD-2019-30444）、Mozilla Firefox 跨站脚本漏洞（CNVD-2019-30446、CNVD-2019-30447）、Mozilla Firefox 类型混淆漏洞。其中，“Mozilla Firefox 资源管理错误漏洞（CNVD-2019-30439、CNVD-2019-30444）”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-2019-30437

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30438

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30439

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30440

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30444

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30446

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30447

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30445

4、F5 产品安全漏洞

F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行非法命令，造成 TMM 重启，导致拒绝服务。

CNVD 收录的相关漏洞包括：F5 BIG-IP 命令注入漏洞（CNVD-2019-30617、CNVD-2019-30625、CNVD-2019-30626）、F5 BIG-IP 输入验证错误漏洞（CNVD-2019-30619、CNVD-2019-30624）、F5 BIG-IP 拒绝服务漏洞（CNVD-2019-30618）、F5 BIG-IP 资源管理错误漏洞、F5 BIG-IP 信息泄露漏洞（CNVD-2019-30623）。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-2019-30617

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30618

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30619

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30621

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30623

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30625

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30626

http://www.cnvd.org.cn/flaw/show/CNVD-2019-30624

5、D-Link DIR-823G 访问控制错误漏洞

D-Link DIR-823G 是一款无线路由器。本周，D-Link DIR-823G 被披露存在访问控制错误漏洞，攻击者可利用该漏洞劫持 WLAN 中所有客户端的 DNS 服务配置信息。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-2019-30424

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-2019-30059	Xymon history.c 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://sourceforge.net/projects/xymon/

CNVD-2019-30149	IBM DB2 High Performance Unload 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-01.ibm.com/support/docview.wss?uid=ibm10964592
CNVD-2019-30256	ZOHO ManageEngine Service Desk Plus 安全特征问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.manageengine.co.uk/products/service-desk/readme.html
CNVD-2019-30485	ESTsoft ALSee 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.estsoft.com/
CNVD-2019-30526	Microsoft Internet Explorer 缓冲区溢出漏洞（CNVD-2019-30526）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0920
CNVD-2019-30710	多款 Huawei 产品版本降级漏洞	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.huawei.com/cn/psirt/security-advisories/huawei-sa-20190904-01-smartphone-cn
CNVD-2019-30717	Varnish Cache 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://varnish-cache.org/security/VSV00003.html
CNVD-2019-30716	Fastjson 远程拒绝服务漏洞	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://github.com/alibaba/fastjson/commit/995845170527221ca0293cf290e33a7d6cb52bf7
CNVD-2019-30736	GOsa 命令执行漏洞	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/gosa-project/gosa-core
CNVD-2019-30737	Brocade Network Advisor 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.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2018-841

小结：本周，Google 被披露存在信息泄露和远程代码执行漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码。此外，Adobe、Mozilla、F5 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过同源策略并获取敏感信息，提升权限，执行任意代码或造成拒绝服务等。另外，D-Link DIR-823G 被披露存在访问控制错误漏洞，攻击者可利用

该漏洞劫持 WLAN 中所有客户端的 DNS 服务配置信息。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、YouPHPTube 远程代码执行漏洞

验证描述

YouPHPTube 是一套基于 PHP 的视频网站系统。

YouPHPTube 存在远程代码执行漏洞。攻击者可利用漏洞执行任意代码。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=33966

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-30053

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. 600000 个 GPS 跟踪器在线曝光，默认密码为“123456”

近日，某安全研究人员透露，一家中国公司生产的至少 600,000 台 GPS 追踪器正在使用相同的默认密码“123456”。黑客可以滥用这个密码劫持用户的帐户，他们可以监视 GPS 跟踪器附近的对话，欺骗跟踪器的真实位置，或者获取跟踪器附加的 SIM 卡电话号码，以便通过 GSM 频道进行跟踪。

参考链接：https://www.zdnet.com/article/600000-gps-trackers-left-exposed-online-with-a-default-password-of-123456/

2. 福建福昕通知客户服务器遭到黑客入侵

福昕 PDF 阅读器和编辑器的开发商福建福昕软通知客户，黑客入侵了它的服务器访问了用户数据。在给受影响客户的邮件通知中，福昕称，未经授权的黑客访问了 My Account 区域。可能访问的用户数据包括了用户名、电邮地址、企业名称、电话号码、用户账号密码和 IP 地址。

参考链接：https://www.cnbeta.com/articles/tech/884469.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