国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 11 月 05 日-2018 年 11 月 11 日 **2018 年第 45 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 172 个，其中高危漏洞 70 个、中危漏洞 89 个、低危漏洞 13 个。漏洞平均分值为 6.30。本周收录的漏洞中，涉及 0day 漏洞 47 个（占 27%），其中互联网上出现“Foscam Opticam i5 栈缓冲区溢出漏洞、Shipping System CMS 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 1228 个，与上周（1005 个）环比增长 18%。

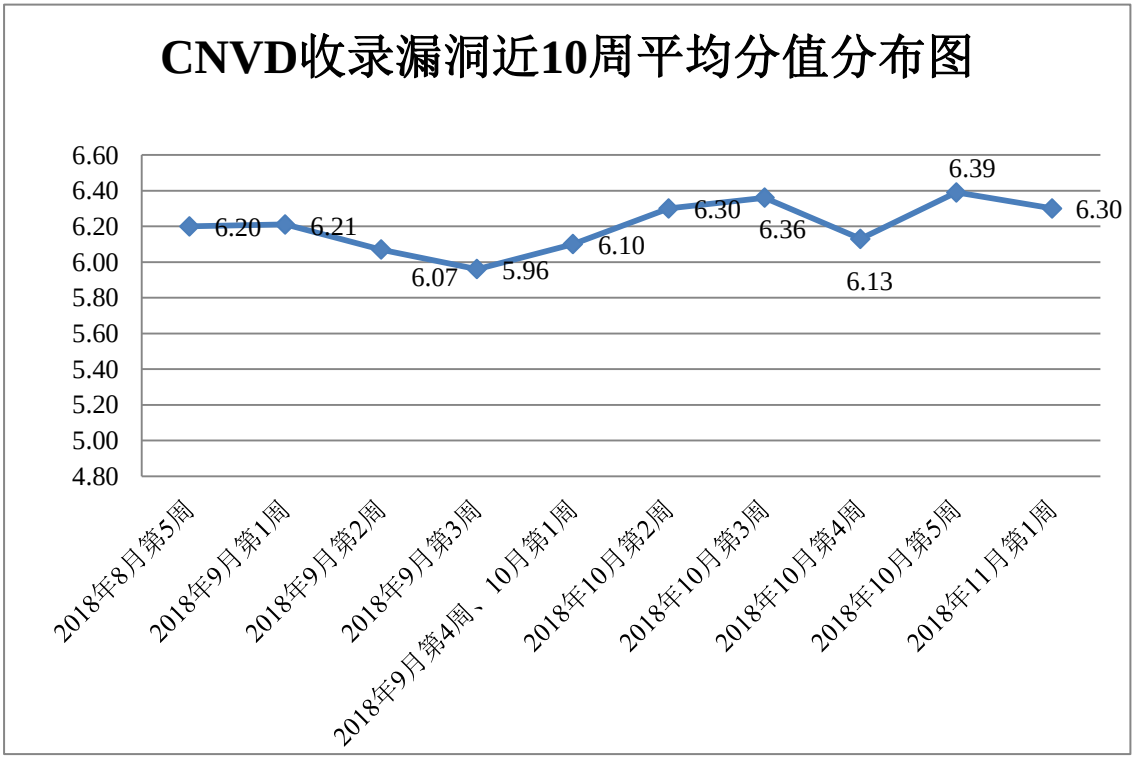

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 0 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 28 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 256 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 60 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 19 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：

灵宝简好网络科技有限公司、上海卓卓网络科技有限公司、哈尔滨伟成科技有限公司、黄石市科威自控有限公司、陕西融达信息科技有限公司 、北京慈记网络科技有限公司、上海岱牧网络有限公司、淄博闪灵网络科技有限公司、长沙翱云网络科技有限公司、洪湖尔创网联信息技术有限公司、上海岱牧网络有限公司、北京海腾时代科技有限公司、成都康菲顿特网络科技有限公司、优肯数位媒体有限公司、北京百容千域软件技术开发有限责任公司、山东有鸿信息科技有限公司、宿迁鑫潮信息技术有限公司、北京后盾计算机技术培训有限责任公司、北京互动百科网络技术股份有限公司、北京江民新科技术有限公司、镇江市云优网络科技有限公司、无锡夸微科技有限公司、北京新启科技有限公司、金山软件股份有限公司、河源市众大文化传媒有限公司、互动在线（北京）科技有限公司、成都九安科技有限公司、苏州联康网络有限公司、阜阳市心品网络科技有限公司、成都龙兵科技有限公司、淇晨科技公司、南京云化通网络科技有限公司、中国电子系统工程第二建设有限公司、南充春杰工作室、地方网络工作室、西安小六网络科技工作室、Zzzcms、信呼、小钱袋、LaySNS、移动物联网实验室、Zcncms、雷风影视、Zzcms、大米 cms、计量学报、Phpyun、HDCMS、视觉江西-中国江西网、中国通信标准化协会。

本周，CNVD 发布了《关于 Apache Struts2 Commons FileUpload 反序列化远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4751

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、北京启明星辰信息安全技术有限公司、哈尔滨安天科技股份有限公司、新华三技术有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京圣博润高新技术股份有限公司、任子行网络技术股份有限公司、中新网络信息安全股份有限公司、河南信安世纪科技有限公司、长春嘉诚信息技术股份有限公司、河北盾安科技有限公司、南京联成科技发展股份有限

公司、内蒙古奥创科技有限公司、上海揆安网络科技有限公司、海南神州希望网络有限公司、山石网科通信技术有限公司、上海启疆信息科技有限公司、北京安码科技有限公司、北京信联科汇科技有限公司、浙江鹏信信息科技股份有限公司及其他个人白帽子向 CNVD 提交了 1228 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 817 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
360 网神（补天平台）	575	575
北京天融信网络安全技术有限公司	334	14
漏洞盒子	242	242
北京启明星辰信息安全技术有限公司	187	21
哈尔滨安天科技股份有限公司	184	0
新华三技术有限公司	150	0
华为技术有限公司	123	0
北京数字观星科技有限公司	55	0
北京神州绿盟科技有限公司	54	0
中国电信集团系统集成有限责任公司	37	0
深信服科技股份有限公司	17	0
恒安嘉新(北京)科技股份公司	14	0
北京知道创宇信息技术有限公司	8	0
沈阳东软系统集成工程有限公司	5	5
山东云天安全技术有限公司	118	118
远江盛邦（北京）网络安全科技股份有限公司	38	38
北京圣博润高新技术股份有限公司	29	29

任子行网络技术股份有限公司	29	29
中新网络信息安全股份有限公司	16	16
河南信安世纪科技有限公司	5	5
长春嘉诚信息技术股份有限公司	4	4
河北盾安科技有限公司	3	3
南京联成科技发展股份有限公司	2	2
内蒙古奥创科技有限公司	2	2
上海揆安网络科技有限公司	2	2
海南神州希望网络有限公司	1	1
山石网科通信技术有限公司	1	1
上海启疆信息科技有限公司	1	1
北京安码科技有限公司	1	1
北京信联科汇科技有限公司	1	1
浙江鹏信信息科技股份有限公司	1	1
CNCERT 山西分中心	7	7
CNCERT 上海分中心	4	4
CNCERT 海南分中心	3	3
CNCERT 内蒙古分中心	3	3
CNCERT 新疆分中心	3	3
CNCERT 浙江分中心	1	1
个人	96	96
报送总计	2356	1228

本周漏洞按类型和厂商统计

本周，CNVD 收录了 172 个漏洞。应用程序漏洞 68 个，操作系统漏洞 62 个，网络设备漏洞 26 个，WEB 应用漏洞 12 个，数据库漏洞 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
应用程序漏洞	68
操作系统漏洞	62
网络设备漏洞	26
WEB 应用漏洞	12
数据库漏洞	4

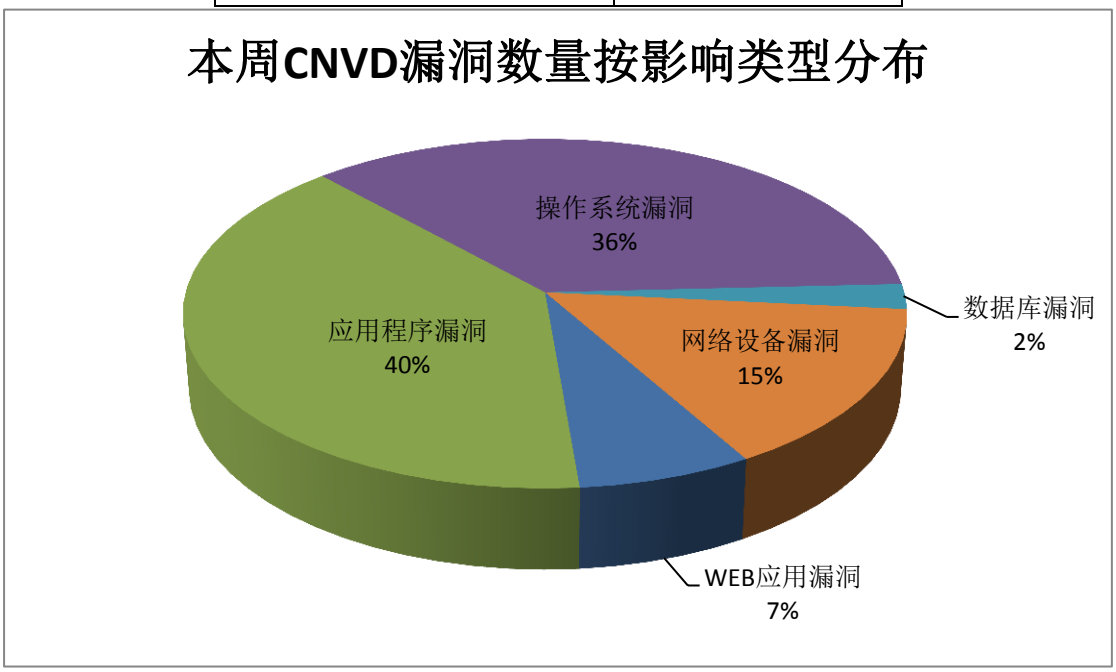

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、IBM、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	Google	49	28%
2	IBM	13	8%
3	Apple	12	7%
4	YI Technology	12	7%
5	Mozilla	8	5%
6	Foscam	7	4%

7	White Shark System	7	4%
8	Apache	4	2%
9	Cisco	4	2%
10	其他	56	33%

本周行业漏洞收录情况

本周，CNVD 收录了 3 个电信行业漏洞，55 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“多款 Apple 产品 Kernel 代码执行漏洞、Cisco WebEx Meetings Server XML 外部实体注入漏洞、Google Android Framework 权限提升漏洞（CNVD-2018-22760）、Apple iOS IOHIDFamily 远程代码执行漏洞”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/

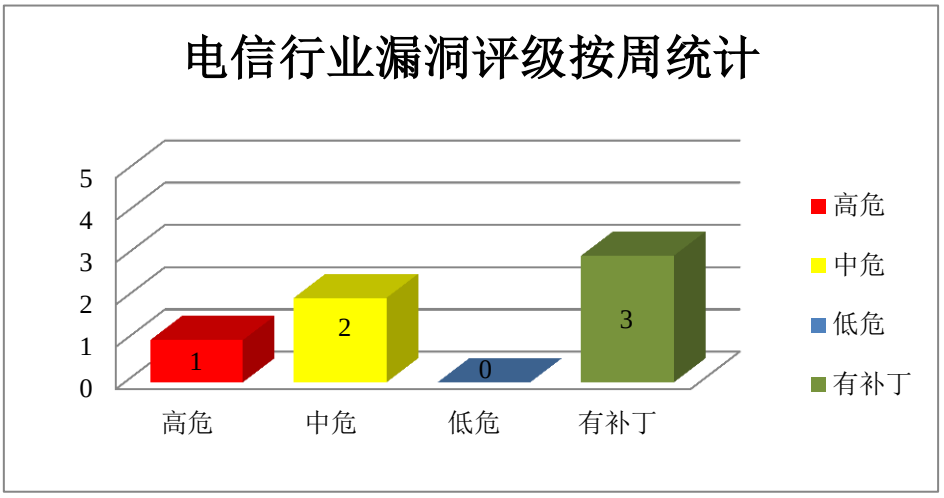

图 3 电信行业漏洞统计

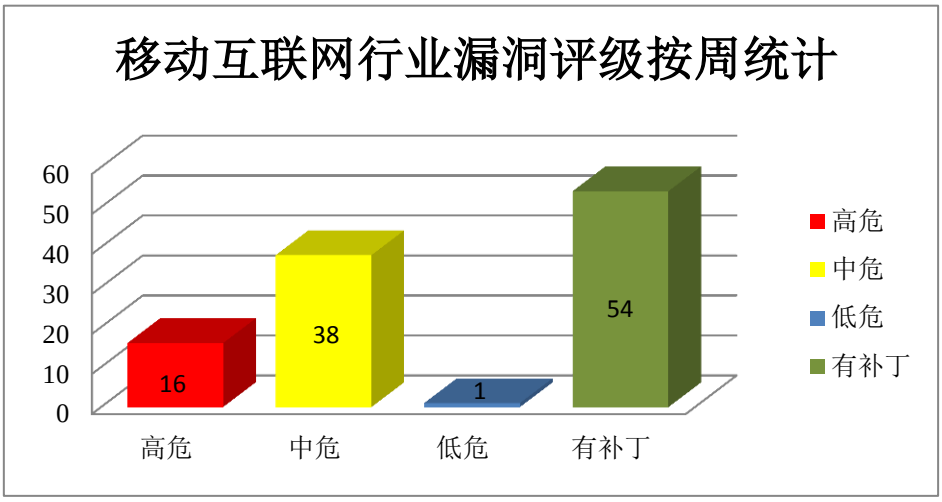

图 4 移动互联网行业漏洞统计

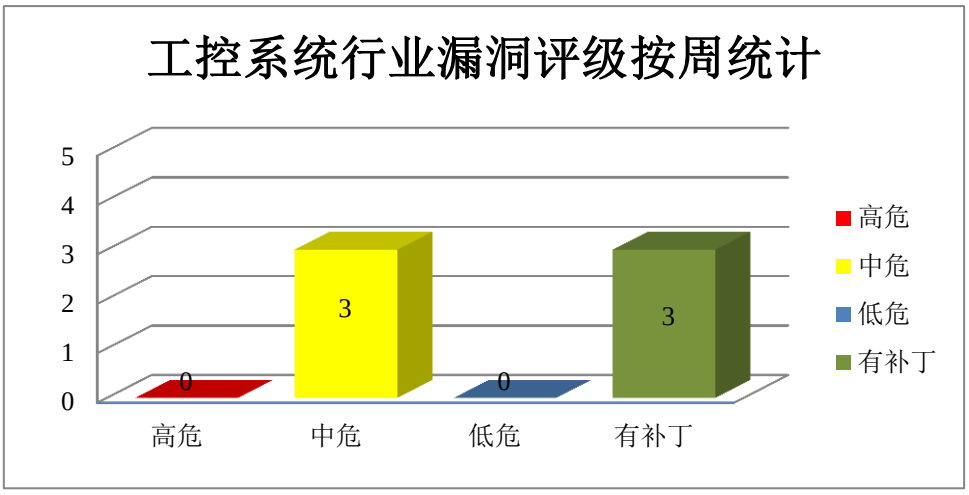

图 5 工控系统行业漏洞统计

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

安卓（Android）是一种基于 Linux 的自由及开放源代码的操作系统，由谷歌公司和开放手机联盟领导及开发。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Framework 权限提升漏洞（CNVD-2018-22761、CNVD-2018-22760、CNVD-2018-22762、CNVD-2018-22763、CNVD-2018-22764、CNVD-2018-22766、CNVD-2018-22765）、Google Android Media framework 权限提升漏洞（CNVD-2018-22767）。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-2018-22761

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22760

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22762

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22763

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22764

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22766

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22765

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22767

2、IBM 产品安全漏洞

IBM Robotic Process Automation with Automation Anywhere 是一套流程自动化解决方案。IBM DB2 是一套关系型数据库管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取 root 访问权限，覆盖系统上的文件，破坏数据库，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Robotic Process Automation with Automation Anywhere 信息泄露漏洞（CNVD-2018-22535、CNVD-2018-22536）、IBM Robotic Process Automation with Automation Anywhere 远程代码执行漏洞、IBM DB2 权限访问控制漏洞、IBM DB2 提权漏洞（CNVD-2018-22924、CNVD-2018-22925、CNVD-2018-22927、CNVD-2018-22926）。其中，“IBM Robotic Process Automation with Automation Anywhere 远程代码执行漏洞、IBM DB2 权限访问控制漏洞、IBM DB2 提权漏洞（CNVD-2018-22925、CNVD-2018-22926）”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-2018-22535

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22536

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22538

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22923

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22924

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22925

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22927

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22926

3、Apple 产品安全漏洞

Apple iOS 是为移动设备所开发的一套操作系统；tvOS 是一套智能电视操作系统；watchOS 是一套智能手表操作系统。Apple macOS Sierra、macOS High Sierra 和 macOS Mojave 都是专为 Mac 计算机所开发的不同版本的专用操作系统。Apple Support for iOS 是一款基于 iOS 系统的在线支持应用程序。本周，上述产品被披露存在多个漏洞，

攻击者可利用漏洞获取敏感信息，以系统权限执行任意代码（内存破坏）。

CNVD 收录的相关漏洞包括：多款 Apple 产品 Kernel 代码执行漏洞、Apple macOS Sierra、macOS High Sierra 和 macOS Mojave dyld 权限提升漏洞、Apple macOS Sierra、macOS High Sierra 和 macOS Mojave IOGraphics 代码执行漏洞、Apple macOS Sierra、macOS High Sierra 和 macOS Mojave Kernel 代码执行漏洞、Apple macOS Mojave Kernel 缓冲区溢出漏洞、Apple macOS High Sierra Grand Central Dispatch 代码执行漏洞、Apple iOS IOHIDFamily 远程代码执行漏洞、Apple Support for iOS Analytics 信息泄露漏洞。其中，除“Apple Support for iOS Analytics 信息泄露漏洞”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-2018-22528
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22530
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22529
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22532
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22531
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22533
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22534
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22570

4、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Firefox ESR 是 Firefox 的一个延长支持版本。Mozilla Firefox for Android 是一款基于 Android 平台的开源 Web 浏览器。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，执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 混合内容漏洞、Mozilla Firefox ESR 存在多个内存破坏漏洞、Mozilla Firefox for Android 信息泄露漏洞、Mozilla Firefox 欺骗漏洞、Mozilla Firefox 和 Firefox ESR 权限提升漏洞、Mozilla Firefox 和 Firefox ESR 未授权访问漏洞、Mozilla Firefox 和 Firefox ESR 任意代码执行漏洞（CNVD-2018-22936、CNVD-2018-22935）。其中，“Mozilla Firefox ESR 存在多个内存破坏漏洞、Mozilla Firefox 和 Firefox ESR 权限提升漏洞、Mozilla Firefox 和 Firefox ESR 任意代码执行漏洞（CNVD-2018-22936、CNVD-2018-22935）”的综合评级为“高危”。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-2018-22929
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22930
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22932
http://www.cnvd.org.cn/flaw/show/CNVD-2018-22931

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22934

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22933

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22936

http://www.cnvd.org.cn/flaw/show/CNVD-2018-22935

5、LiquidVPN For macOS 权限提升漏洞

LiquidVPN For MacOS 是一款基于 MacOS 平台的用于匿名访问互联网的 VPN 软件。本周，LiquidVPN For MacOS 被披露存在权限提升漏洞。攻击者可利用该漏洞获取提升的权限。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-2018-22844

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-2018-22522	Cisco WebEx Meetings Server XML 外部实体注入漏洞	高	用户可联系供应商获得补丁信息：http://cisco.com
CNVD-2018-22524	Dell OpenManage Network Manager 授权不当漏洞	高	用户可联系供应商获得补丁信息：https://www.dell.com/support/article/us/en/19/sln314610
CNVD-2018-22525	Zoho ManageEngine OpManager SQL 注入漏洞（CNVD-2018-22525 ）	高	用户可联系供应商获得补丁信息：https://www.manageengine.com
CNVD-2018-22641	多款 Huawei 手机认证绕过漏洞	高	华为已发布版本修复该漏洞，安全预警链接：http://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20181101-01-bypass-cn
CNVD-2018-22749	Pale Moon 内存错误引用漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.palemoon.org/releasenotes.shtml
CNVD-2018-22756	Cisco Meraki Local Status Page 权限提升漏洞	高	思科发布了解决此漏洞的软件更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181107-meraki
CNVD-2018-22759	Micro Focus Operation Bridge Containerized Suite 远程代码执行漏洞	高	用户可联系供应商获得补丁信息：https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03283416
CNVD-2018-22758	Cisco Stealthwatch Management Console 份验证绕过漏洞	高	思科发布了解决此漏洞的软件更新：https://tools.cisco.com/security/center/c

			ontent/CiscoSecurityAdvisory/cisco-sa-20181107-smc-auth-bypass
CNVD-2018-22776	Yi Home Camera 信息泄露漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.yitechnology.com/
CNVD-2018-22938	Apache Superset 命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/apache/incubator-superset/pull/4243

小结：本周，Google 被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。此外，IBM、Apple、Mozilla 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，以系统权限执行任意代码（内存破坏）等。另外，LiquidVPN For MacOS 被披露存在权限提升漏洞。攻击者可利用该漏洞获取提升的权限。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、Foscam Opticam i5 栈缓冲区溢出漏洞

验证描述

Foscam Opticam i5 是福斯康姆(FOSCAM)推出的一款 IP 摄像机。

系统固件为 1.5.2.11 和应用程序固件为 2.21.1.128 的 Foscam Opticam i5 的 ONVIF devicemgmt SetDNS 方法存在栈缓冲区溢出漏洞。远程攻击者可通过 IPv4Address 字段利用该漏洞导致栈缓冲区溢出。

验证信息

POC 链接：https://sintonen.fi/advisories/foscam-ip-camera-multiple-vulnerabilities.txt

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-22822

信息提供者

华为技术有限公司

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. Windows VBScript 引擎 RCE 漏洞

VBScript 引擎处理内存中对象的方式中存在一个远程执行代码漏洞。该漏洞可能以

一种攻击者可以在当前用户的上下文中执行任意代码的方式来破坏内存。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后攻击者可以安装程序；查看，更改或删除数据；或创建具有完全用户权限的新帐户。

参考链接：https://www.anquanke.com/post/id/163841

2. GPU 存在边信道攻击漏洞，可用于间谍监控和密码窃取

某研究人员近日表示，攻击者可利用计算机的图形处理单元（GPU）来监视网络活动、窃取密码并入侵基于云的应用程序。他们还逆向了一个英伟达 GPU 来演示对图形和计算堆栈的三种攻击。这三种攻击都需要先让受害者感染嵌入在下载应用中的恶意程序，进而监听受害者的计算机。随后，通过监听用户键入字符的间隔时间等信息，获取到用户密码。最后，针对云上计算应用程序，在 GPU 上启动恶意工作载荷，与受害者的应用程序一起运行。最后根据神经网络参数、缓存等内容，在性能计数跟踪器上使用基于机器学习的分类手段，提取受害者的秘密神经网络结构等信息。目前，英伟达已经接收到漏洞信息并表示将发布补丁。

参考链接：https://www.helpnetsecurity.com/2018/11/06/gpu-side-channel-attacks/

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