# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2019 年 11 月 18 日-2019 年 11 月 24 日** **2019 年第 47 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 494 个，其中高危漏洞 147 个、中危漏洞 285 个、低危漏洞 62 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 145 个（占 29%），其中互联网上出现“Apache mod_ssl 远程缓冲区溢出漏洞、YouPHPTube SQL 注入漏洞（CNVD-2019-41830）”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 2044 个，与上周（7452 个）环比减少 73%。

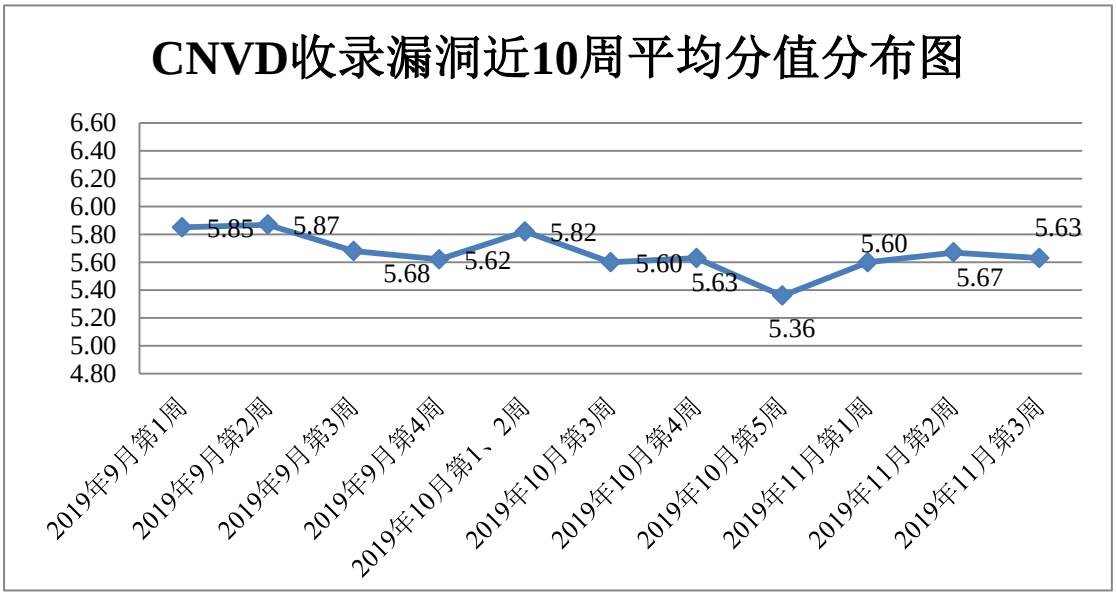


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 14 起，向基础电信企业通报漏洞事件 8 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 540 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 53 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 25 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：

四平市九州易通科技有限公司、深圳市中联创新自控系统有限公司、杭州双收网络技术有限公司、金山软件股份有限公司、湖南潭州教育网络科技有限公司、深圳市天地心网络技术有限公司、北京良精科技有限公司、成都康菲顿特网络科技有限公司、中粮集团有限公司、湖南考试在线网络科技有限公司、伽然信息科技（上海）有限公司、淄博闪灵网络科技有限公司、山西先启科技有限公司、北京良精志诚科技有限责任公司、宿迁鑫潮信息技术有限公司、国核电力规划设计研究院有限公司、成都鹏博士电信传媒集团股份有限公司、昆明云涛科技有限公司、深圳市迪元素科技有限公司、正方软件股份有限公司、嘉兴想天信息科技有限公司、国投电力控股股份有限公司、山西牛酷信息科技有限公司、徐州安信网络科技有限公司、南京博纳睿通软件科技有限公司、湖南壹拾捌号网络技术有限公司、北京堆栈科技有限公司、广州联雅网络科技有限公司、深圳市蓝色航线科技有限公司、上海商创网络科技有限公司、上海泛微网络科技股份有限公司、洛阳云业信息科技有限公司、厦门凤凰创壹软件有限公司、搜狐公司、深圳市迅雷网络技术有限公司、河北晨光网络科技有限公司、北京信用达互联网信息技术有限公司、北京融智创想信息技术有限公司、北京对啊网教育科技有限公司、飞狐信息技术（天津）有限公司、塔迈（广州）信息技术有限公司、重庆楚捷科技有限公司、杭州趣维科技有限公司、广联达科技股份有限公司、上海麦克风文化传媒有限公司、上海流利说信息技术有限公司、北京智者天下科技有限公司、小咖秀（北京）科技有限公司、北京外研在线数字科技有限公司、深圳迪元素科技有限公司、乐尚商城开源系统、海洋 CMS、海城市忠华资讯网络发展中心、中国文化产业协会、Jeeplus、The Apache Software Foundation、Xnview、奥壹科技（OE）团队、人人影视、超级 CMS 和 ShopXO。

本周，CNVD 发布了《关于云存储应用存在越权访问和文件上传漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5291

## 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、哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、深信服科技股份有限公司、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、北京铭图天成信息技术有限公司、山东新潮信息技术有限公司、北京华云安信息

技术有限公司、杭州海康威视数字技术股份有限公司、南京众智维信息科技有限公司、山东云天安全技术有限公司、杭州迪普科技股份有限公司、广州蕴辰网络科技有限公司、山东华鲁科技发展股份有限公司、北京君信安科技有限公司、山石网科通信技术股份有限公司、河南信安世纪科技有限公司、内蒙古奥创科技有限公司、江苏保旺达软件技术有限公司、腾讯安全云鼎实验室、北京智游网安科技有限公司、国瑞数码零点实验室、清远职业技术学院、中通服咨询设计研究院有限公司及其他个人白帽子向 CNVD 提交了 2044 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 1389 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 |
|---|---|---|
| 阿里云计算有限公司 | 1082 | 0 |
| 奇安信网神（补天平台） | 706 | 706 |
| 斗象科技（漏洞盒子） | 413 | 413 |
| 上海交大 | 270 | 270 |
| 哈尔滨安天科技集团股份有限公司 | 178 | 0 |
| 北京天融信网络安全技术有限公司 | 164 | 0 |
| 深信服科技股份有限公司 | 118 | 1 |
| 华为技术有限公司 | 96 | 0 |
| 厦门服云信息科技有限公司 | 92 | 2 |
| 恒安嘉新(北京)科技股份公司 | 61 | 0 |
| 新华三技术有限公司 | 56 | 0 |
| 北京神州绿盟科技有限公司 | 37 | 0 |
| 中国电信集团系统集成有限责任公司 | 22 | 22 |
| 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 | 16 | 16 |
| 四川无声信息技术有限公司 | 9 | 9 |

| | | |
|---|---|---|
| 北京启明星辰信息安全技术有限公司 | 8 | 8 |
| 北京知道创宇信息技术股份有限公司 | 4 | 0 |
| 南京联成科技发展股份有限公司 | 3 | 3 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 99 | 99 |
| 北京铭图天成信息技术有限公司 | 86 | 86 |
| 山东新潮信息技术有限公司 | 54 | 54 |
| 北京华云安信息技术有限公司 | 34 | 34 |
| 杭州海康威视数字技术股份有限公司 | 31 | 31 |
| 南京众智维信息科技有限公司 | 23 | 23 |
| 山东云天安全技术有限公司 | 17 | 17 |
| 杭州迪普科技股份有限公司 | 15 | 1 |
| 广州蕴辰网络科技有限公司 | 6 | 6 |
| 山东华鲁科技发展股份有限公司 | 6 | 6 |
| 北京君信安科技有限公司 | 5 | 5 |
| 山石网科通信技术股份有限公司 | 5 | 5 |
| 河南信安世纪科技有限公司 | 4 | 4 |
| 内蒙古奥创科技有限公司 | 3 | 3 |
| 江苏保旺达软件技术有限公司 | 2 | 2 |
| 腾讯安全云鼎实验室 | 2 | 2 |
| 北京智游网安科技有限公司 | 1 | 1 |
| 国瑞数码零点实验室 | 1 | 1 |
| 清远职业技术学院 | 1 | 1 |

| | | |
|---|---|---|
| 中通服咨询设计研究院有限公司 | 1 | 1 |
| CNCERT 宁夏分中心 | 11 | 11 |
| CNCERT 贵州分中心 | 4 | 4 |
| 个人 | 197 | 197 |
| 报送总计 | 3963 | 2044 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 494 个漏洞。应用程序 222 个，WEB 应用 98 个，操作系统 98 个，网络设备（交换机、路由器等网络端设备）40 个，智能设备（物联网终端设备）23 个，安全产品 13 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 | 222 |
| WEB 应用 | 98 |
| 操作系统 | 98 |
| 网络设备（交换机、路由器等网络端设备） | 40 |
| 智能设备（物联网终端设备） | 23 |
| 安全产品 | 13 |

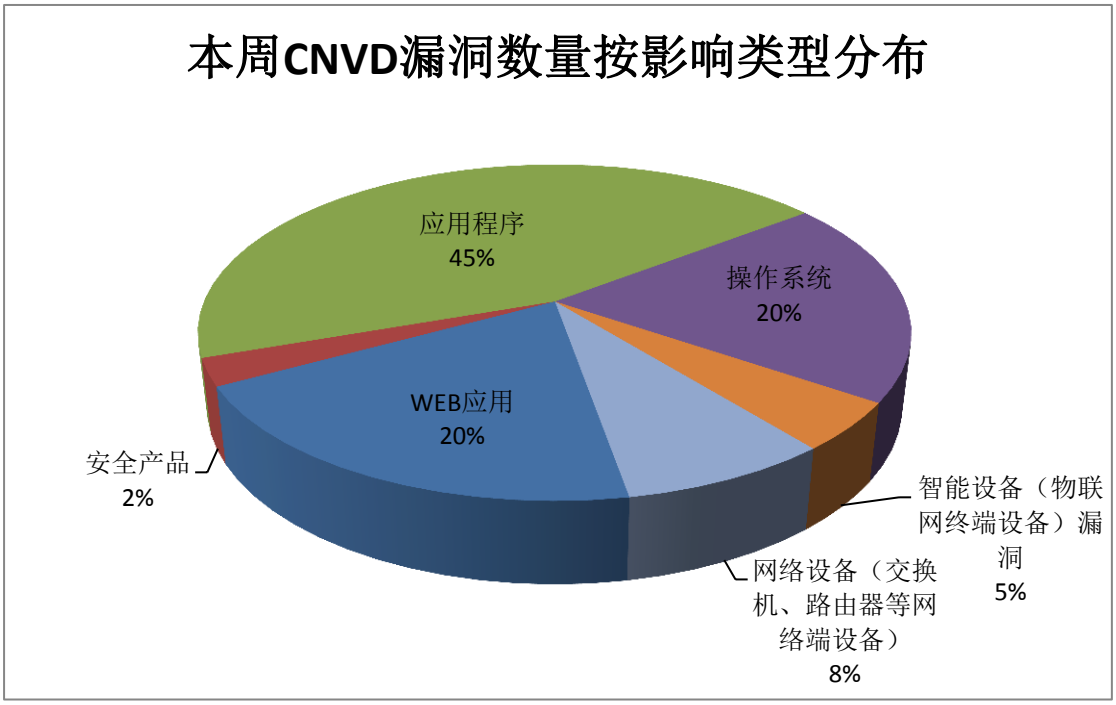


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Linux、Apache、TYPO3 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 | Linux | 41 | 8% |
| 2 | Apache | 23 | 5% |
| 3 | TYPO3 | 22 | 5% |
| 4 | Tcpdump | 21 | 4% |
| 5 | Google | 17 | 3% |
| 6 | JetBrains | 16 | 3% |
| 7 | Intel | 15 | 3% |
| 8 | Juniper Networks | 15 | 3% |
| 9 | Apple | 15 | 3% |
| 10 | 其他 | 309 | 63% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，58 个移动互联网行业漏洞，21 个工控行业漏洞（如下图所示）。其中，“多款 Siemens 产品拒绝服务漏洞（CNVD-2019-41280）、多款 Apple 产品 Audio 组件内存破坏漏洞、Linux kernel 内存泄露漏洞（CNVD-2019-41709）、Google Android System 组件信息泄露漏洞（CNVD-2019-41735）、Valleylab FT 10 和 Valleylab FX8 输入验证错误漏洞”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/

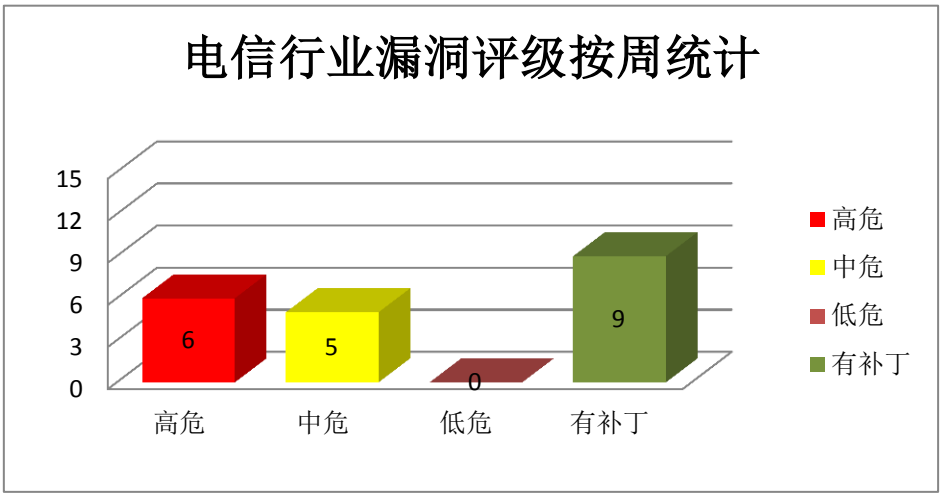


图 3 电信行业漏洞统计

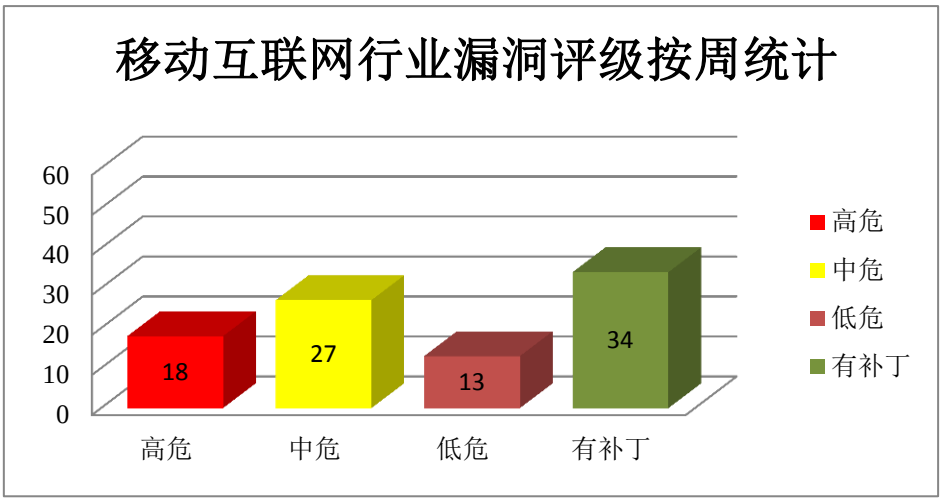


图 4 移动互联网行业漏洞统计

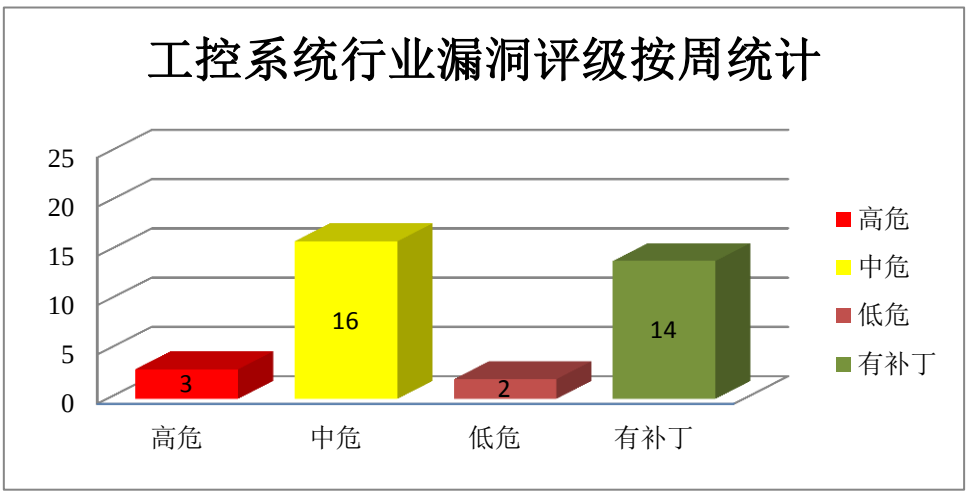


图 5 工控系统行业漏洞统计

## 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、Apache 产品安全漏洞

Apache Solr 是一款基于 Lucene（一款全文搜索引擎）的搜索服务器。Apache Guacamole 是一款无客户端的远程桌面网关。Apache Thrift 是一种接口定义语言和二进制通信协议，用于为多种语言定义和创建服务。Apache Traffic Server 是一套可扩展的 HTTP 代理和缓存服务器。Apache Hadoop 是一套开源的分布式系统基础架构。Apache MINA 是一款网络应用程序框架。Apache Atlas 是一个可扩展的核心基础治理服务集，使企业能够高效地满足 Hadoop 中的合规性要求，并允许与整个企业数据生态系统集成。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，绕过安全限制并执行未授权的操作，执行客户端代码，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Apache Solr 认证绕过漏洞、Apache Guacamole 信息泄露漏洞、Apache Thrift 越界读取漏洞、Apache Traffic Server sslheader 插件信息泄露漏洞、Apache Hadoop 缓冲区溢出漏洞、Apache CXF OpenId connect token 服务信息泄露漏洞、Apache MINA 内存破坏漏洞、Apache Atlas 存储型跨站脚本漏洞。其中，“Apache Solr 认证绕过漏洞、Apache CXF OpenId connect token 服务信息泄露漏洞”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-2019-41284
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41285
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41289
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41292
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41851
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41853
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41852
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41855

## 2、Huawei 产品安全漏洞

Huawei P30、Mate 9 Pro、AR1200 和 P20 等都是中国华为（Huawei）公司的一款智能手机。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受影响组件敏感信息，执行恶意代码等。

CNVD 收录的相关漏洞包括：Huawei P30、Huawei P30 Pro 和 Honor Princeton-AL10B 条件竞争漏洞、Huawei Mate 9 Pro 信息泄露漏洞（CNVD-2019-41253）、多款 Huawei 产品 FRP 绕过漏洞、多款 Huawei 产品数字签名校验绕过漏洞、Huawei Emily-L29C 信息泄露漏洞、Huawei P20 访问控制不当漏洞、Huawei P20 文件管理不当漏洞、Huawei P30、Mate 20 和 P30 Pro 缓冲区溢出漏洞。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-2019-41252

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41253
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41255
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41256
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41257
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41258
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41259
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41838

### 3、Google 产品安全漏洞

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）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多个漏洞，攻击者可利用漏洞提升权限，执行代码。

CNVD 收录的相关漏洞包括：Google Android System 组件提权漏洞、Google Android System 组件缓冲区溢出漏洞（CNVD-2019-41732）、Google Android System 组件信息泄露漏洞（CNVD-2019-41735）、Google Android Framework 组件权限提升漏洞（CNVD-2019-41736、CNVD-2019-41737）、Google Android Library 缓冲区溢出漏洞、Google Android 缓冲区溢出漏洞（CNVD-2019-41738）、Google Android 权限提升漏洞（CNVD-2019-41901）。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-2019-41731
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41732
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41735
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41736
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41737
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41739
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41738
http://www.cnvd.org.cn/flaw/show/CNVD-2019-41901

### 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内存泄露漏洞，攻击者可利用漏洞造成拒绝服务（内存消耗）。

CNVD 收录的相关漏洞包括：Linux kernel 内存泄露漏洞（CNVD-2019-41709、CNVD-2019-41710、CNVD-2019-41711、CNVD-2019-41712、CNVD-2019-41713、CNVD-2019-41714、CNVD-2019-41716、CNVD-2019-41717）。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-2019-41709

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41710

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41711

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41712

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41713

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41714

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41716

http://www.cnvd.org.cn/flaw/show/CNVD-2019-41717

**5、IBM Maximo Asset Management 权限提升漏洞**

IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。该方案能够在一个平台上管理所有类型的资产，如设施、交通运输等，并对这些资产实现单点控制。本周，IBM Maximo Asset Management 被披露存在权限提升漏洞。攻击者可利用该漏洞删除无权限删除的记录。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-2019-41617

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-2019-41280 | 多款 Siemens 产品拒绝服务漏洞（CNVD-2019-41280） | 高 | 目前厂商发布了部分产品的升级补丁以修复漏洞，详情请参考链接：https://cert-portal.siemens.com/productcert/pdf/ssa-349422.pdf |
| CNVD-2019-41462 | Intel Ethernet 700 Series Controllers 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://downloadcenter.intel.com/product/46828/700-Series-Network-Adapters-up-to-40GbE- |
| CNVD-2019-41473 | Juniper Networks Junos OS 授权问题漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10960&actp=METADATA |
| CNVD-2019-41622 | Adobe Media Encoder 越界写入漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/media-encoder/apsb19-52.html |
| CNVD-2019-41639 | Microsoft Windows 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://portal.msrc.microsoft.com/zh-C |

| | | | |
|---|---|---|---|
| | | | N/security-guidance/advisory/CVE-2019-1430 |
| CNVD-2019-41644 | Symantec Endpoint Protection 代码执行漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.symantec.com/us/en/article.SYMSA1488.html |
| CNVD-2019-41645 | IBM UrbanCode Deploy 文件下载漏洞 | 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.ibm.com/support/pages/node/1107249 |
| CNVD-2019-41688 | Fortinet FortiClient 权限提升漏洞（CNVD-2019-41688） | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/psirt/FG-IR-19-238 |
| CNVD-2019-41898 | ZTE ZXHN F670 命令注入漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010163 |
| CNVD-2019-41911 | tcpdump 缓冲区溢出漏洞（CNVD-2019-41911） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/the-tcpdump-group/tcpdump/blob/tcpdump-4.9/CHANGES |

小结：本周，Apache 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，绕过安全限制并执行未授权的操作，执行客户端代码，导致缓冲区溢出或堆溢出等。此外，Huawei、Google、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取受影响组件敏感信息，提升权限，执行恶意代码，造成拒绝服务（内存消耗）等。另外，IBM Maximo Asset Management 被披露存在权限提升漏洞。攻击者可利用该漏洞删除无权限删除的记录。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 SQL 注入漏洞（CNVD-2019-41830）

**验证描述**

YouPHPTube 是一套基于 PHP 的视频网站系统。

YouPHPTube 7.2 版本中的 userCreate.json.php 文件存在 SQL 注入漏洞。该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令。

**验证信息**

POC 链接：https://www.exploit-db.com/exploits/47294

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2019-41830

**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. Google Chrome 实验功能导致浏览器标签崩溃

Google Chrome 的一项实验功能导致浏览器标签发生崩溃，全世界有大量企业受波及。问题持续了两天，没有影响所有 Chrome 用户，而是主要影响运行在 Windows Server terminal server 设置——这是企业网络中非常常见的设置——下的 Chrome 浏览器。数以百计的用户通过 Google 支持论坛报告，雇员使用的 Chrome 标签突然变成空白，这一错误被称为“白屏死亡”。

参考链接：https://www.solidot.org/story?sid=62625

### 2. 谷歌三星安卓摄像头应用含高危漏洞变身监控器，影响数亿设备

近日，某安全研究团队的研究人员表示，任何应用程序在不具备具体权限的情况下均可控制谷歌的安卓摄像头 app 并强制其拍照和/或录视频，即使手机锁定且屏幕关闭的情况也不例外。该团队将研究结果告知谷歌，后者通知了其它安卓厂商，其中三星已确认其智能手机中也存在这些漏洞。谷歌指出其它原始设备制造厂商也确认了这些漏洞的存在，影响全球数亿台设备。该团队在报告中说明的是从 Pixel 2 和 Pixel 3 设备上找到的漏洞，不过谷歌所有的手机模型均存在这些被统称为 CVE-2019-2234 的漏洞问题。

参考链接：https://www.freebuf.com/vuls/220644.html

**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