# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2019 年 02 月 11 日-2019 年 02 月 17 日** **2019 年第 7 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 218 个，其中高危漏洞 62 个、中危漏洞 129 个、低危漏洞 27 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 84 个（占 39%），其中互联网上出现“VyOS 权限提升漏洞、Zyxel NBG-418N v2 Modem 跨站请求伪造漏洞”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 1058 个，与上周（1761 个）环比下降 40%。

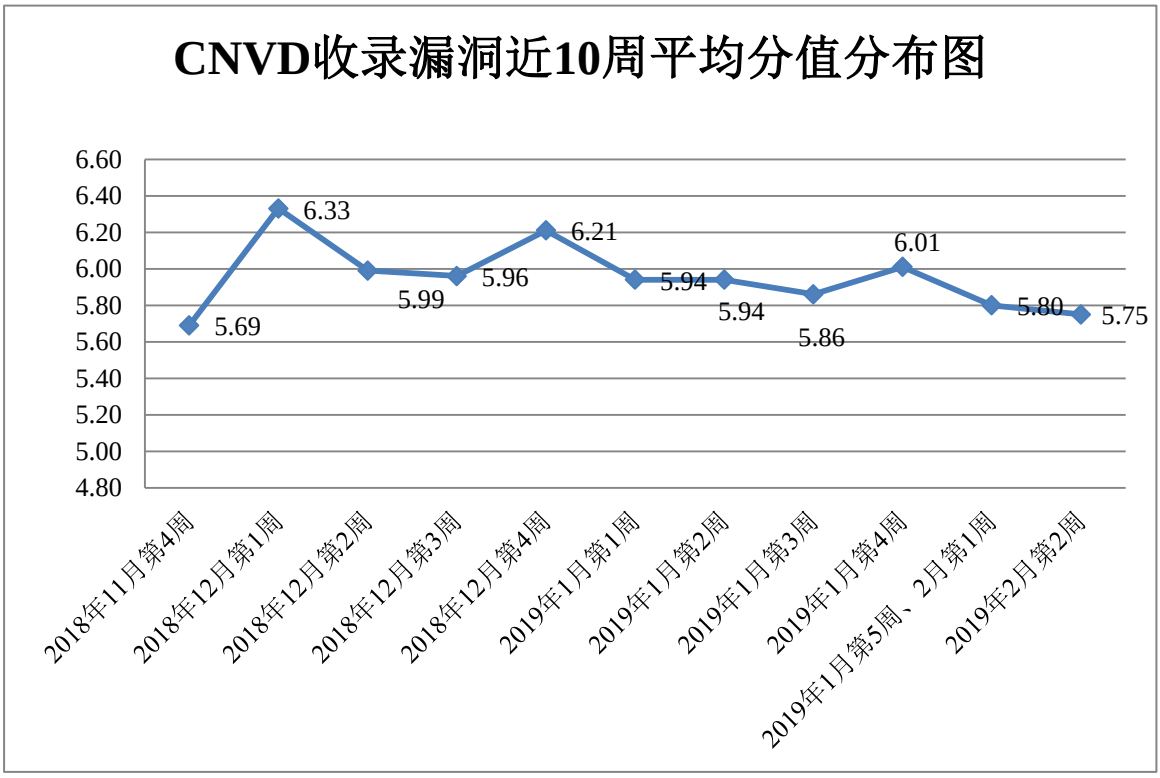


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 36 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 235 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 72 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 18 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：

青岛易软天创网络科技有限公司、宿迁鑫潮信息技术有限公司、飞利浦（中国）投资有限公司、珠海金山办公软件有限公司、湖南翱云网络科技有限公司、上海鹏达计算机系统开发有限公司、北京展招网络技术有限公司、上海企望信息科技有限公司、上海商创网络科技有限公司、嘉兴想天信息科技有限公司、成都思乐科技有限公司、福州极限软件开发有限公司、上海丹帆网络科技有限公司、重庆韬龙网络科技有限公司、深圳市沃仕达科技有限公司、山东至信信息科技有限公司、成都康菲顿特网络科技有限公司、泰州智搜网络科技有限公司、安徽启明星工作室、中国国防工业企业协会军民融合产业联盟、小二胡工作室、长沙市天心区斌网网络技术服务部、中国生态文化协会、SemCms、Jymusic、CatfishCMS、XYCMS 和大米 CMS。

本周，CNVD 发布了《Microsoft 发布 2019 年 2 月安全更新》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4893

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、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、新华三技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。天津市国瑞数码安全系统股份有限公司、中新网络信息安全股份有限公司、南京联成科技发展股份有限公司、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、重庆贝特计算机系统工程有限公司、河南信安世纪科技有限公司、山东华鲁科技发展股份有限公司、山石网科通信技术股份有限公司、北京百卓网络技术有限公司、内蒙古奥创科技有限公司、远江盛邦（北京）网络安全科技股份有限公司及其他个人白帽子向 CNVD 提交了 1058 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 687 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） | 407 | 407 |

| | | |
|---|---|---|
| 斗象科技（漏洞盒子） | 280 | 280 |
| 华为技术有限公司 | 173 | 0 |
| 哈尔滨安天科技集团股份有限公司 | 142 | 0 |
| 北京天融信网络安全技术有限公司 | 118 | 5 |
| 新华三技术有限公司 | 117 | 0 |
| 北京神州绿盟科技有限公司 | 91 | 0 |
| 四川无声信息技术有限公司 | 60 | 60 |
| 北京启明星辰信息安全技术有限公司 | 36 | 1 |
| 北京数字观星科技有限公司 | 24 | 0 |
| 中国电信集团系统集成有限责任公司 | 17 | 0 |
| 恒安嘉新(北京)科技股份公司 | 16 | 0 |
| 西安四叶草信息技术有限公司 | 6 | 6 |
| 北京知道创宇信息技术有限公司 | 5 | 0 |
| 沈阳东软系统集成工程有限公司 | 1 | 1 |
| 天津市国瑞数码安全系统股份有限公司 | 79 | 79 |
| 中新网络信息安全股份有限公司 | 29 | 29 |
| 南京联成科技发展股份有限公司 | 26 | 26 |
| 山东云天安全技术有限公司 | 15 | 15 |
| 任子行网络技术股份有限公司 | 10 | 10 |
| 重庆贝特计算机系统工程有限公司 | 6 | 6 |
| 河南信安世纪科技有限公司 | 3 | 3 |
| 山东华鲁科技发展股份有限公司 | 3 | 3 |

| | | |
|---|---|---|
| 山石网科通信技术股份有限公司 | 2 | 2 |
| 北京百卓网络技术有限公司 | 1 | 1 |
| 内蒙古奥创科技有限公司 | 1 | 1 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 1 | 1 |
| CNCERT 甘肃分中心 | 6 | 6 |
| CNCERT 吉林分中心 | 6 | 6 |
| CNCERT 上海分中心 | 3 | 3 |
| CNCERT 贵州分中心 | 1 | 1 |
| CNCERT 内蒙古分中心 | 1 | 1 |
| 个人 | 105 | 105 |
| 报送总计 | 1791 | 1058 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 218 个漏洞。应用程序漏洞 122 个，操作系统漏洞 39 个，网络设备漏洞 38 个，WEB 应用漏洞 19 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 | 122 |
| 操作系统漏洞 | 39 |
| 网络设备漏洞 | 38 |
| WEB 应用漏洞 | 19 |

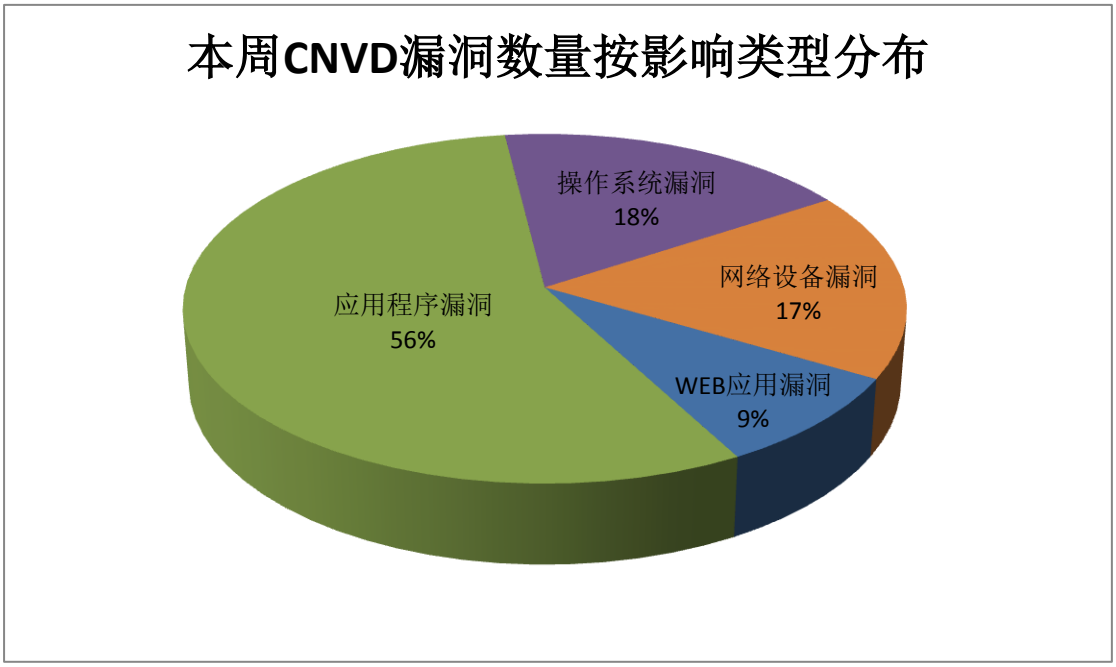


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Adobe、D-Link 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 | Microsoft | 32 | 15% |
| 2 | Adobe | 21 | 10% |
| 3 | D-Link | 20 | 9% |
| 4 | Foscam | 13 | 6% |
| 5 | WordPress | 12 | 6% |
| 6 | Apple | 11 | 5% |
| 7 | Micco | 5 | 2% |
| 8 | Cantata | 4 | 2% |
| 9 | ACD Systems | 3 | 1% |
| 10 | 其他 | 97 | 44% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 22 个电信行业漏洞，11 个移动互联网行业漏洞（如下图所示）。其中，“D-Link DIR-823G 无需验证重启漏洞、Apple iOS GasGauge 内存破坏漏洞（CNVD-2019-04302）”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/

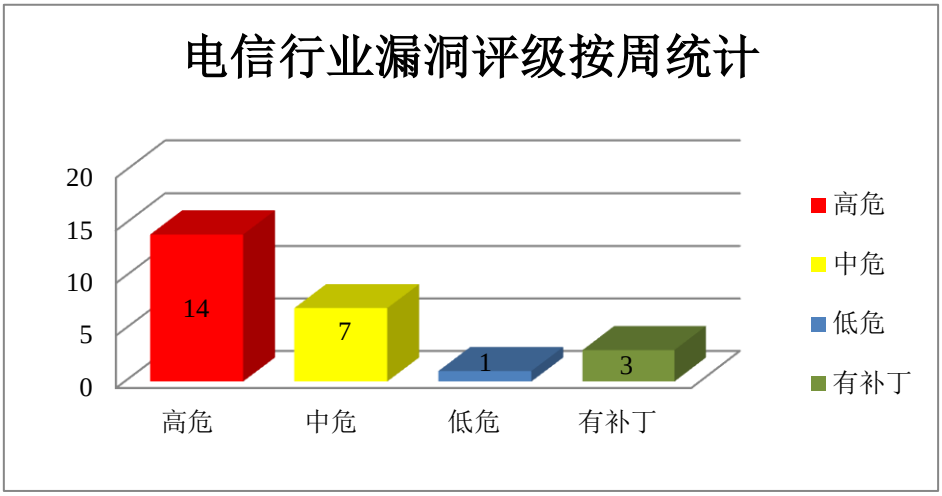


图 3 电信行业漏洞统计

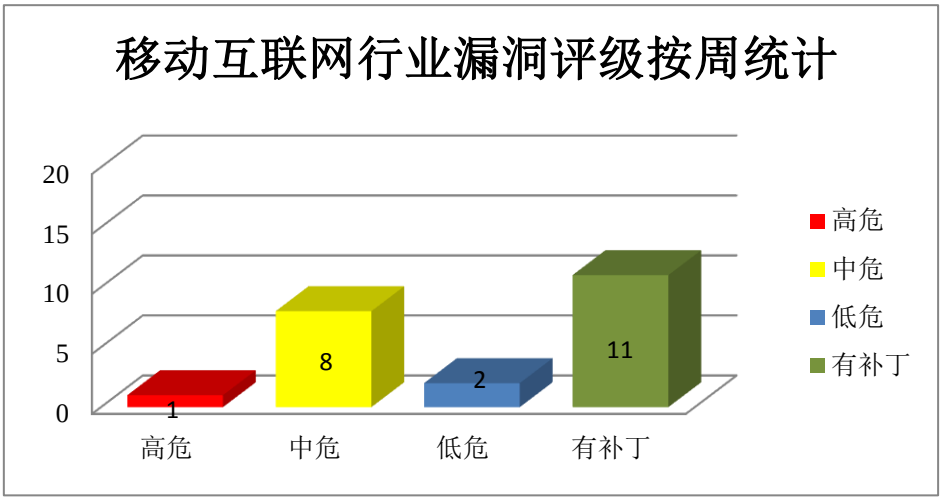


图 4 移动互联网行业漏洞统计

## 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、Microsoft 产品安全漏洞

Microsoft Windows 10 等都是美国微软（Microsoft）公司发布的一系列操作系统。Windows Domain Name System（DNS）是其中的一套域名系统服务器。Microsoft Windows 10 是一套个人电脑使用的操作系统。Windows Server 2016 是一套服务器操作系统。Microsoft Internet Explorer（IE）是一款 Web 浏览器，是 Windows 操作系统附带的默认浏览器。Microsoft .NET Framework 是一种全面且一致的编程模型。Visual Studio 是开发

工具包系列产品。Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。JET Database Engine 是其中的一个数据库引擎。本周，上述产品被披露存在远程代码执行和远程内存破坏漏洞，攻击者可利用漏洞执行任意代码，造成内存破坏。

CNVD 收录的相关漏洞包括：Microsoft Windows Domain Name System 远程代码执行漏洞、Microsoft Windows 远程代码执行漏洞（CNVD-2019-03928）、Microsoft Internet Explorer 远程内存破坏漏洞（ CNVD-2019-04150）、Microsoft .NET Framework 和 Visual Studio 远程代码执行漏洞、Microsoft Windows JET Database Engine 远程代码执行漏洞（CNVD-2019-04154、CNVD-2019-04155、CNVD-2019-04157、CNVD-2019-04156）。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-2019-03927
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03928
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04150
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04153
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04154
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04155
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04157
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04156

**2、Adobe 产品安全漏洞**

Adobe Acrobat 是一套 PDF 文件编辑和转换工具，Adobe Reader 是一套 PDF 文档阅读软件。本周，上述产品被披露存在任意代码执行和越界读取漏洞，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：Adobe Acrobat 和 Reader 任意代码执行漏洞（CNVD-2019-03932、CNVD-2019-03934）、Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2019-03938、CNVD-2019-03939、CNVD-2019-03940、CNVD-2019-03941、CNVD-2019-03942、CNVD-2019-03943）。其中，“Adobe Acrobat 和 Reader 任意代码执行漏洞（CNVD-2019-03932、CNVD-2019-03934）”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-2019-03932
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03934
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03938
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03939
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03940
http://www.cnvd.org.cn/flaw/show/CNVD-2019-03941

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03942

http://www.cnvd.org.cn/flaw/show/CNVD-2019-03943

### 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；Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。WebKit 是其中的一个 Web 浏览器引擎组件。Apple mac OS Sierra 是为 Mac 计算机所开发的一套专用操作系统。macOS High Sierra 是它的下一代产品。Hypervisor（又名虚拟机器监视器，VMM）是一个运行在物理服务器和操作系统之间的中间软件层，它可允许多个操作系统和应用共享一套基础物理硬件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞伪造地址栏内容，提升权限，执行任意代码（内核破坏），造成 ASSERT 失败等。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 拒绝服务漏洞（CNVD-2019-04295、CNVD-2019-04296）、Apple macOS Sierra 和 macOS High Sierra Hypervisor 权限提升漏洞、Apple macOS Sierra 和 macOS High Sierra Intel Graphics Driver 内存破坏漏洞、Apple iOS SafariViewController 地址栏欺骗漏洞、Apple iOS ReplayKit 类型混淆漏洞、Apple iOS GasGauge 内存破坏漏洞（CNVD-2019-04302）、Apple iOS Calculator 未授权操作漏洞。其中，“Apple macOS Sierra 和 macOS High Sierra Hypervisor 权限提升漏洞、Apple macOS Sierra 和 macOS High Sierra Intel Graphics Driver 内存破坏漏洞、Apple iOS GasGauge 内存破坏漏洞（CNVD-2019-04302）”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-2019-04295

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04296

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04298

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04299

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04300

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04301

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04302

http://www.cnvd.org.cn/flaw/show/CNVD-2019-04303

### 4、D-Link 产品安全漏洞

D-Link DIR-619L Rev.B、DIR-605L Rev.B、DVA-5592、DCM-604、DCM-704、DIR-823G、DIR-600M C1 和 DIR-878 都是（D-Link）公司的路由器产品。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，绕过身份验证，访问路由器控制面板，执行任意代码。

CNVD 收录的相关漏洞包括：D-Link DIR-619L 和 DIR-605L 栈缓冲区溢出漏洞、

D-Link DVA-5592 认证绕过漏洞、D-Link DCM-604 和 DCM-704 信息泄露漏洞、D-Link DCM-604 和 DCM-704 凭证泄露漏洞、D-Link DIR-823G 命令注入漏洞、D-Link DIR-600M 认证绕过漏洞、D-Link DIR-878 命令注入漏洞（CNVD-2019-04290、CNVD-2019-04292）。其中，除“D-Link DCM-604 和 DCM-704 信息泄露漏洞、D-Link DCM-604 和 DCM-704 凭证泄露漏洞、D-Link DIR-823G 命令注入漏洞”外，其余漏洞的综合评级为“高危”。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-2019-04181
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04199
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04198
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04202
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04200
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04201
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04290
http://www.cnvd.org.cn/flaw/show/CNVD-2019-04292

### 5、Foscam C2 和 Opticam i5 操作系统命令注入漏洞

Foscam C2 和 Opticam i5 都是中国福斯康姆（FOSCAM）公司的网络摄像机产品。本周，Foscam C2 和 Opticam i5 设备被披露存在操作系统命令注入漏洞。远程攻击者可借助‘modelName’参数中的 shell 元字符利用该漏洞执行任意 OS 命令。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-2019-04045

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-2019-03778 | IBM Financial Transaction Manager for ACH Services SQL 注入漏洞 | 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=ibm10869520 |
| CNVD-2019-03780 | ACD Systems Canvas Draw 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.acdsystems.com/ |
| CNVD-2019-03890 | POWER EGG 执行命令漏洞 | 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://jvn.jp/en/jp/JVN63860183/ |
| CNVD-2019-03891 | rssh 远程命令执行漏洞 | 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://www.debian.org/security/2019/dsa-4382 |
| CNVD-2019-03898 | phpMyAdmin 本地文件包含漏洞 | 高 | 用户可联系供应商获得补丁信息：https://www.phpmyadmin.net/ |
| CNVD-2019-04134 | Geutebrück E2 Camera Series 操作系统命令注入漏洞 | 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://www.geutebrueck.com/en_EN.html |
| CNVD-2019-04137 | Ubuntu Linux 本地提权漏洞（CNVD-2019-04137） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.ubuntu.com/ |
| CNVD-2019-04143 | EMC VNX2 OS 命令注入漏洞 | 高 | 用户可联系供应商获得补丁信息：https://seclists.org/fulldisclosure/2019/Feb/8 |
| CNVD-2019-04307 | Axentra Hipserv NAS OS 未认证远程命令执行漏洞 | 高 | 用户可联系供应商获得补丁信息：http://www.axentra.com/en/ |
| CNVD-2019-04305 | Nexus Repository Manager 3 远程代码执行漏洞 | 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://support.sonatype.com/hc/en-us/articles/360017310793-CVE-2019- |

小结：本周，Google 被披露存在权限提升和拒绝服务漏洞，攻击者可利用漏洞提升权限，造成拒绝服务。此外，Apple、HDF5、HPE 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，执行任意代码（内存破坏），造成堆缓冲区越界读取，发起拒绝服务攻击等。另外，Technicolor DPC3928SL 被披露存在跨站脚本漏洞。远程攻击者可借助 setSSID 利用该漏洞注入任意的 Web 脚本或 HTML。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、Zyxel NBG-418N v2 Modem 跨站请求伪造漏洞

**验证描述**

Zyxel NBG-418N v2 Modem 是一款无线路由器。

Zyxel NBG-418N v2 Modem 1.00(AAXM.6)C0 版本中存在跨站请求伪造漏洞，远程攻击者可利用该漏洞执行未授权的操作。

**验证信息**

POC 链接：https://www.exploit-db.com/exploits/46240

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-03785

**信息提供者**

恒安嘉新(北京)科技股份公司

*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. Ubuntu Snap 软件包存在漏洞，允许攻击者获得系统 Root 权限

安全研究员在 Canonical 的 REST API 中发现了一个漏洞，snapd 守护程序可允许攻击者获取 Linux 系统的 root 访问权限。Canonical 是 Ubuntu Linux 的软件包提供商之一，一直以来都在推广他们的“Snap”软件包，将所有应用程序依赖项转换为单个二进制文件（类似于 Windows 应用程序）。Snap 环境包括一个“应用程序商店”，开发人员可以在其中贡献和维护现成的软件包，其中一个名为 snapd 服务用于本地安装管理和在线商店通信。漏洞就来自这个服务，名为为’Dirty_Sock’的漏洞会影响安装了 Ubuntu Linux 的服务器，专家在 Ubuntu 上成功测试并发布概念验证，展示如何提升权限。

参考链接：https://securityaffairs.co/wordpress/81059/hacking/snapd-privilege-escalation.html

### 2. 微软产品七成漏洞是内存安全问题

微软工程师 Matt Miller 在以色列举行的安全会议 BlueHat 上透露，软件巨人旗下产品过去 12 年修复的所有漏洞，七成涉及的是内存安全问题。内存安全是软件和安全工程师使用的术语，描述应用程序以不会导致错误的方式访问操作系统内存。当软件无意或有意以超出其分配大小和内存地址的方式访问内存时，就会出现内存安全漏洞。缓冲区溢出、竞争条件、分页错误、空指针，堆栈耗尽，堆耗尽/损坏、释放后使用或双重释放等术语描述的都是内存安全漏洞。

参考链接：https://www.solidot.org/story?sid=59556

### 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