# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

**2019 年 03 月 25 日-2019 年 03 月 31 日** **2019 年第 13 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 269 个，其中高危漏洞 93 个、中危漏洞 153 个、低危漏洞 23 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 130 个（占 48%），其中互联网上出现“ABUS Secvest FUBE50014 和 ABUS Secvest FUBE50015 拒绝服务漏洞、WordPress wp-bs3-rad Themes 任意文件上传漏洞”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 1960 与上周（1788 个）环比增长 10%

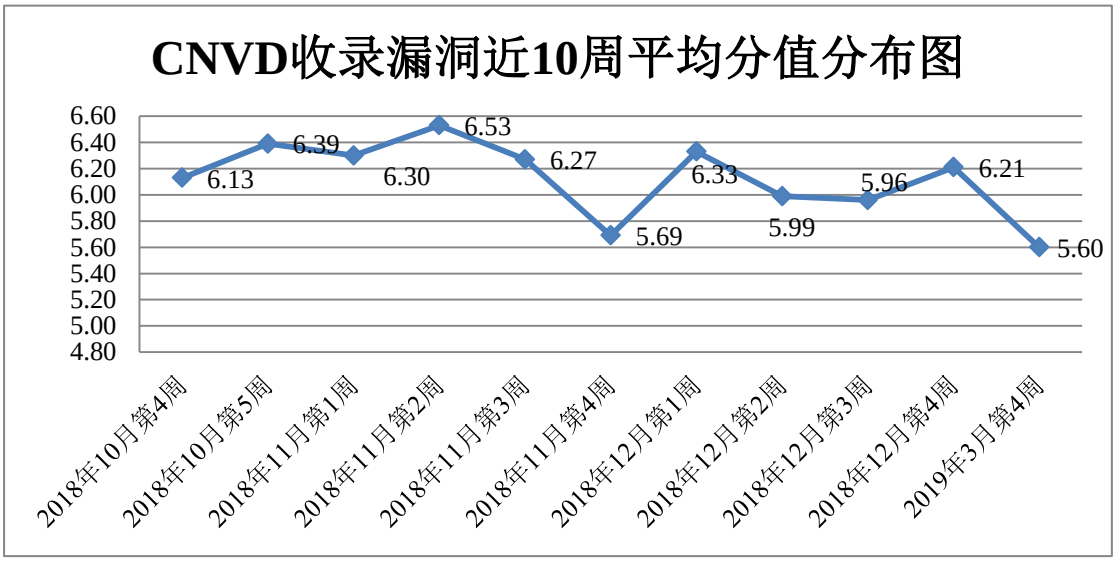


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 7 起，向银行、保险、能源等重要行业单位通报漏洞事件 23 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 456 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 40 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：

湖南潭州教育网络科技有限公司、北京十度创想科技有限公司、浙江齐治科技股份有限公司、太原迅易科技有限公司、郑州大象通信信息技术有限公司、广州拓波软件科技有限公司、北京城市联盟科技有限公司、金山软件股份有限公司、成都康菲顿特网络科技有限公司、杭州可道云网络有限公司、深圳迪元素科技有限公司、杭州海康威视数字技术股份有限公司、上海卓卓网络科技有限公司、西安三才科技实业有限公司、佛山市云迈电子商务有限公司、上海茸易科技有限公司、北京博乐虎科技有限公司、西安蓝色海岸信息技术有限公司、微软(中国)有限公司、澳通（大连）科技发展有限公司、四三九九网络股份有限公司、北京亿赛通科技发展有限责任公司、易校通软件科技、信呼、智睿软件、鑫跃科技、海通网络、云阳工作室、米酷资源网、耳朵软件、海洋 CMS、SEMCMS、SocuSoft、Earcms、CSZ-CM、zzzcms。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，沈阳东软系统集成工程有限公司、尔滨安天科技集团股份有限公司、京天融信网络安全技术有限公司、为技术有限公司、华三技术有限公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、东九州信泰信息科技股份有限公司、新网络信息安全股份有限公司、徽锋刃信息科技有限公司、春嘉诚信息技术股份有限公司、京圣博润高新技术股份有限公司、京长亭科技有限公司、东华鲁科技发展股份有限公司、子行网络技术股份有限公司、南信安世纪科技有限公司、京国舜科技股份有限公司、蒙古奥创科技有限公司、东云天安全技术有限公司、西网信信息安全等级保护测评有限公司、石网科通信技术股份有限公司、国交通通信信息中心、庆市信息通信咨询设计院有限公司、海玄猫信息科技有限公司、庆贝特计算机系统工程有限公司及其他个人白帽子向 CNVD 提交了 1960 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 1347 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） | 840 | 840 |
| 360 网神（补天平台） | 507 | 507 |
| 沈阳东软系统集成工程有限公司 | 440 | 0 |
| 哈尔滨安天科技集团股份有限公司 | 264 | 0 |

| | | |
|---|---|---|
| 北京天融信网络安全技术有限公司 | 223 | 7 |
| 华为技术有限公司 | 119 | 0 |
| 新华三技术有限公司 | 98 | 0 |
| 北京数字观星科技有限公司 | 77 | 0 |
| 北京启明星辰信息安全技术有限公司 | 65 | 8 |
| 深信服科技股份有限公司 | 60 | 0 |
| 四川无声信息技术有限公司 | 58 | 58 |
| 北京神州绿盟科技有限公司 | 42 | 0 |
| 中国电信集团系统集成有限责任公司 | 41 | 0 |
| 恒安嘉新(北京)科技股份公司 | 34 | 0 |
| 北京知道创宇信息技术有限公司 | 14 | 11 |
| 厦门服云信息科技有限公司 | 6 | 0 |
| 西安四叶草信息技术有限公司 | 6 | 6 |
| 国瑞数码零点实验室 | 137 | 137 |
| 山东九州信泰信息科技股份有限公司 | 54 | 54 |
| 中新网络信息安全股份有限公司 | 53 | 53 |
| 安徽锋刃信息科技有限公司 | 36 | 36 |
| 长春嘉诚信息技术股份有限公司 | 31 | 31 |
| 北京圣博润高新技术股份有限公司 | 21 | 21 |
| 北京长亭科技有限公司 | 10 | 10 |
| 山东华鲁科技发展股份有限公司 | 6 | 6 |
| 任子行网络技术股份有限公司 | 6 | 6 |

| | | |
|---|---|---|
| 河南信安世纪科技有限公司 | 5 | 5 |
| 北京国舜科技股份有限公司 | 4 | 4 |
| 内蒙古奥创科技有限公司 | 4 | 4 |
| 山东云天安全技术有限公司 | 4 | 4 |
| 广西网信信息安全等级保护测评有限公司 | 3 | 3 |
| 山石网科通信技术股份有限公司 | 2 | 2 |
| 中国交通通信信息中心 | 2 | 2 |
| 重庆市信息通信咨询设计院有限公司 | 2 | 2 |
| 上海玄猫信息科技有限公司 | 1 | 1 |
| 重庆贝特计算机系统工程有限公司 | 1 | 1 |
| CNCERT 河北分中心 | 5 | 5 |
| CNCERT 四川分中心 | 4 | 4 |
| CNCERT 北京分中心 | 2 | 2 |
| CNCERT 西藏分中心 | 2 | 2 |
| CNCERT 海南分中心 | 1 | 1 |
| CNCERT 云南分中心 | 1 | 1 |
| CNCERT 浙江分中心 | 1 | 1 |
| 个人 | 125 | 125 |
| 报送总计 | 3417 | 1960 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 269 洞。应用程序漏洞 148 个，WEB 应用漏洞 87 个，操作系统漏洞 17 个，网络设备漏洞 15 个，安全产品漏洞 2 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 | 148 |
| WEB 应用漏洞 | 87 |
| 操作系统漏洞 | 17 |
| 网络设备漏洞 | 15 |
| 安全产品漏洞 | 2 |

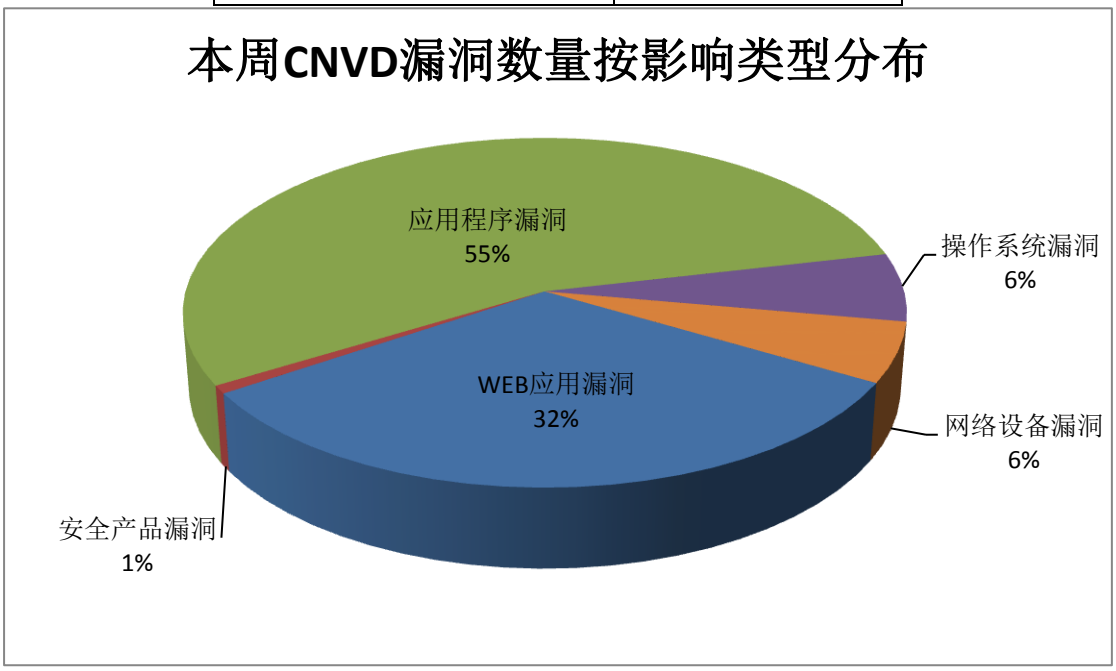


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、SAP、WordPress 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 | Mozilla | 23 | 9 |
| 2 | SAP | 20 | 7% |
| 3 | WordPress | 15 | 6% |
| 4 | Apple | 14 | 5% |
| 5 | Samba | 10 | 4% |
| 6 | Foxit | 9 | 3% |
| 7 | OFCMS | 9 | 3% |
| 8 | Cisco | 6 | 2% |
| 9 | Micro Focus | 6 | 2% |
| 10 | 其他 | 157 | 58% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，25 个移动互联网行业漏洞，1 个工控行业漏洞，（如下图所示）。其中，“Apple iOS、tvOS 和 macOS Mojave Kernel 缓冲区溢出漏洞、Cisco IOS 和 IOS XE 输入验证漏洞、Apple iOS、tvOS 和 macOS Mojave Kernel 越界读取漏洞、PostgreSQL 任意代码执行漏洞”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/

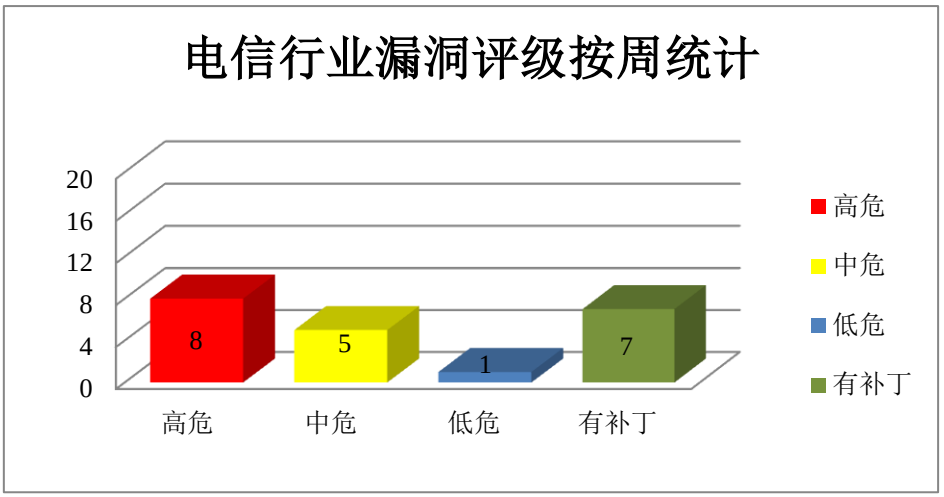


图 3 电信行业漏洞统计

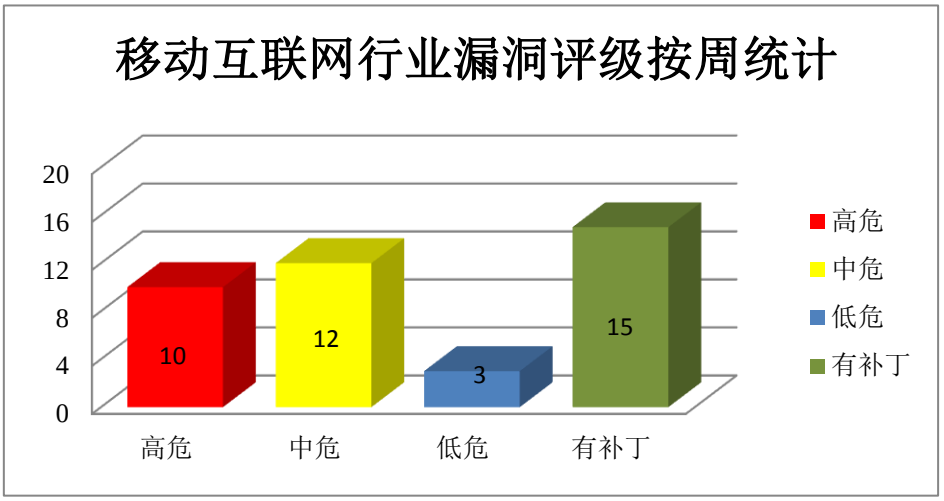


图 4 移动互联网行业漏洞统计

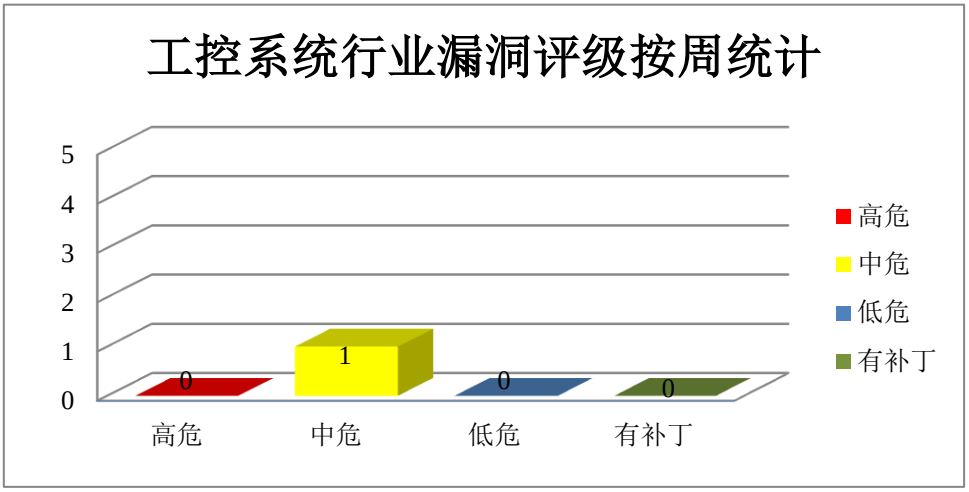


图 5 控系统行业漏洞统计

## 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、Apple 产品安全漏洞

Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。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 iOS 是为移动设备所开发的一套操作系统。Apple tvOS 是一套智能电视操作系统。Apple Safari 是一款 Web 浏览器，是 MacOSX 和 iOS 操作系统附带的默认浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码（内存破坏）。

CNVD 收录的相关漏洞包括：Apple macOS Mojave PackageKit 权限提升漏洞、Apple macOS Mojave AppleGraphicsControl 缓冲区溢出漏洞、Apple iCloud for Windows iCloud Installer 代码执行漏洞、Apple iOS、tvOS 和 macOS Mojave Kernel 越界读取漏洞、多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2019-08709、CNVD-2019-08712）、Apple iOS、tvOS 和 macOS Mojave Kernel 缓冲区溢出漏洞、多款 Apple 产品 WebKit 内存错误引用漏洞（CNVD-2019-08714）。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-2019-08568

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08567

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08569

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08707

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08709

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08712

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08711

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08714

**2、Mozilla 产品安全漏洞**

Mozilla Firefox 是一款开源 Web 浏览器。Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。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或造成拒绝服务（崩溃）等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR 内存错误引用漏洞（CNVD-2019-08521）、Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2019-08523）、Mozilla Firefox 内存破坏漏洞（CNVD-2019-08522）、Mozilla Firefox 和 Firefox ESR 命令执行漏洞（CNVD-2019-08525）、Mozilla Firefox 和 Firefox ESR IonMonkey JIT 编译器内存破坏漏洞、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2019-08529）、Mozilla Firefox Firefox Developer Tools 代码执行漏洞、Mozilla Firefox 内存破坏漏洞（CNVD-2019-08540）。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-2019-08521

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08523

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08522

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08525

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08527

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08529

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08538

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08540

**3、Foxit 产品安全漏洞**

Foxit Reader for Windows 是一款基于 Windows 平台的 PDF 文档阅读器。Phantom PDF for Windows 是它的商业版。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息，执行任务代码。

CNVD 收录的相关漏洞包括：Foxit Reader 和 PhantomPDF 内存错误引用漏洞（CNVD-2019-08300、CNVD-2019-08302）、Foxit Reader 和 PhantomPDF 输入验证漏洞（CNVD-2019-08301、CNVD-2019-08303）、Foxit Reader 和 PhantomPDF 越界读取漏洞、Foxit Reader 和 PhantomPDF 信息泄露漏洞（CNVD-2019-08304）、Foxit Reader 越界读漏洞（CNVD-2019-08306）、Foxit Reader setInterval 方法内存错误引用漏洞。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-2019-08300

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08302

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08301

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08303

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08305

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08304

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08306

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08307

### 4、Samba 产品安全漏洞

Samba 是一套可使 UNIX 系列的操作系统与微软 Windows 操作系统的 SMB/CIFS 网络协议做连结的自由软件。该软件支持共享打印机、互相传输资料文件等。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，未授权访问资源，执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Samba 访问绕过漏洞、Samba 拒绝服务漏洞（CNVD-2019-08284、CNVD-2019-08285、CNVD-2019-08293、CNVD-2019-08297）、Samba 安全绕过漏洞（CNVD-2019-08286）、Samba 内存破坏漏洞、Samba 远程拒绝服务漏洞（CNVD-2019-08296）。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-2019-08283

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08284

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08285

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08286

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08287

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08293

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08296

http://www.cnvd.org.cn/flaw/show/CNVD-2019-08297

### 5、Adrenalin eSystems HRMS Software 跨站脚本漏洞

Adrenalin eSystems HRMS Software 是一套人力资源管理系统。Adrenalin eSystems HRMS Software 被披露存在跨站脚本漏洞。远程攻击者可借助‘ReportId’参数利用该漏洞注入恶意的 JavaScript 代码。参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-08275

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-2019-08272 | Pivotal Software Concourse SQL 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://pivotal.io/security/cve-2019-3792 |
| CNVD-2019-08279 | PostgreSQL 任意代码执行漏洞 | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：http://paper.tuisec.win/detail/66d2b3ec28c7239 |
| CNVD-2019-08291 | IBM Sterling B2B Integrator XML 外部实体注入漏洞（CNVD-2019-08291） | 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/docview.wss?uid=ibm10874238 |
| CNVD-2019-08292 | Dell EMC NetWorker 远程代码执行漏洞 | 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://www.dellemc.com/ |
| CNVD-2019-08311 | ArcSight Logger 远程代码执行漏洞（CNVD-2019-08311） | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://softwaresupport.softwaregrp.com/doc/KM03355866 |
| CNVD-2019-08338 | QNAP QTS 缓冲区溢出漏洞（CNVD-2019-08338） | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://www.qnap.com/zh-tw/security-advisory/nas-201811-22 |
| CNVD-2019-08352 | Apache Heron 路径遍历漏洞 | 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/apache/incubator-heron |
| CNVD-2019-08461 | Cisco SPA514G 拒绝服务漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190313-sip |
| CNVD-2019-08491 | EDK2 缓冲区溢出漏洞 | 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/tianocore/edk2 |
| CNVD-2019-08539 | Huawei Hima-AL00B 代码执行漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20190320-01-phone-cn |

小结：本周，Apple 被披露存在存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码（内存破坏）。此外，Mozilla、Foxit、Samba 等多款产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息，绕过安全限制，未授权访问资源，执行任意代码或发起拒绝服务攻击等。另外，Adrenalin eSystems HRMS Software 被披露存在跨站脚本漏洞。远程攻击者可借助‘ReportId’参数利用该漏洞注入恶意的 JavaScript 代码。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、ABUS Secvest FUBE50014 和 ABUS Secvest FUBE50015 拒绝服务漏洞

**验证描述**

ABUS Secvest FUBE50014 和 ABUS Secvest FUBE50015 都是德国 ABUS 公司的一款无线遥控器。

ABUS Secvest FUBE50014 和 ABUS Secvest FUBE50015 中存在安全漏洞，该漏洞源于程序未加密信号通信并且使用了易被猜测到的滚动码。攻击者可利用该漏洞造成拒绝服务。

**验证信息**

POC 链接：https://packetstormsecurity.com/files/152218/ABUS-Secvest-Remote-Control-Denial-Of-Service.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-08179

**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. UC 浏览器存在中间人攻击(MITM)漏洞，可能影响十多亿设备

研究人员发现 UC 浏览器中存在易受攻击的功能模块，可被攻击者利用执行中间人攻击。由于 UC 浏览器采用 HTTP 协议与服务器通信，传输的信息没有经过加密，所以会被攻击者 hook 来自应用程序的请求，并将命令和链接替换为恶意地址，导致从 UC 浏览器下载模块时，会下载来自恶意服务器的内容。而 UC 浏览器本身使用未签名的插件，因此没有任何验证就可能启动恶意模块。攻击者可以利用这种机制，使用 UC 浏览器分发、执行不同的恶意插件，甚至利用木马访问受保护的浏览器文件并窃取存储在程序目录中的密码。UC 浏览器有十几亿下载量，相关设备都可能暴露在风险之中。

参考链接：https://www.bleepingcomputer.com/news/security/uc-browser-for-android-desktop-exposes-500-million-users-to-mitm-attacks/

### 2. 新发现的 HTTPS 漏洞可能会使您的数据暴露在外

意大利威尼斯 CA’Foscari 大学和奥地利 Tu Wien 大学的研究人员发现，超过 100

00 个使用 HTTPS 的顶级网站仍然容易受到传输层安全漏洞的攻击。当用户访问这些网站时，HTTPS 的绿色挂锁锁仍然会出现在地址栏中。TLS 中的错误很难被检测到，但它们仍然存在，攻击者可以使用这些漏洞来解密来自 cookie 的信息。虽然 cookie 不会向攻击者提供任何敏感信息，但还有其他缺陷。攻击者可以访问浏览器和服务器之间交换的几乎所有数据。

参考链接：https://secgroup.github.io/tlswebscan/

## 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