# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2018 年 9 月 24 日-2018 年 10 月 7 日　　2018 年第39、40 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 267 个，其中高危漏洞 93 个、中危漏洞 168 个、低危漏洞 6 个。漏洞平均分值为 6.10。本周收录的漏洞中，涉及 0day 漏洞 100 个（占 37%），其中互联网上出现“LG SuperSign CMS 远程代码执行漏洞、Joomla!组件 Penny Auction Factory 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 1261 个，与上周（588 个）环比增长 1.14 倍。

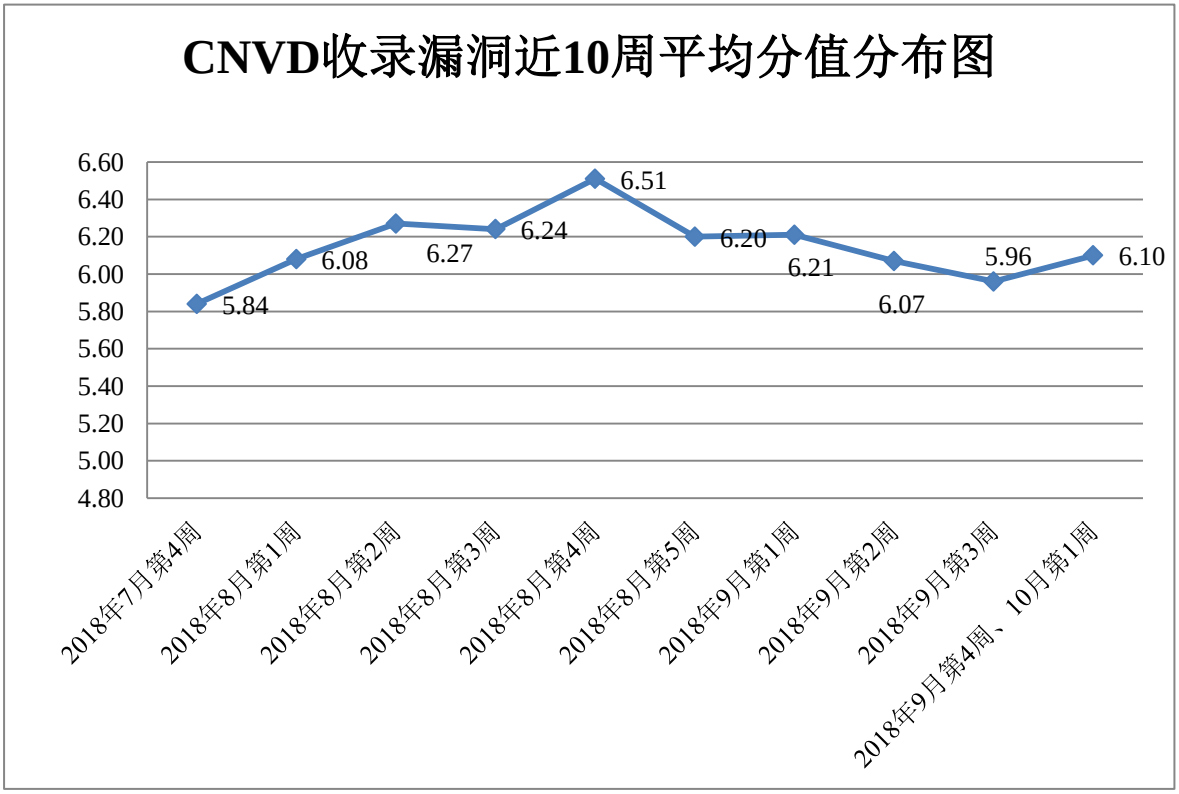


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 12 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 349 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 69 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 31 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：

深圳市锟铻科技有限公司、镇江市云优网络科技有限公司、连云港捷铁国际货运代理有限公司、辽宁畅通数据通信有限公司、上海顶倍信息科技有限公司、北京江民新科技术有限公司、上海金电网安科技有限公司、北京宝通投资集团有限公司、北京尚睿通网络科技有限公司、深圳普汇斯科技有限公司、宿迁鑫潮信息技术限公司、上海明一通讯技术有限公司、上海亿速网络科技有限公司、北京五指互联科技有限公司、聊城市领胜网络科技有限公司、深圳市博思协创网络科技有限公司、深圳市快金数据技术服务有限公司、金山软件股份有限公司、河南中科建筑规划设计有限公司、中国化学工程集团有限公司、中粮集团有限公司、广州无线电集团有限公司、北京小米科技有限责任公司、南京玻璃纤维研究设计院有限公司、闻泰网络、宜软通网、中南汽车教育网、中国招教网、中国肝健康网、中华板报网、北京东方时尚驾校、中国园林绿化行业协会、中国药学会、中华口腔医学研究杂志、中国产权交易所、中图科技、大米 CMS、SemCms、Gxlcms、CatfishCMS、BANDISOFT、PHPEMS。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技股份有限公司、蓝盾信息安全技术有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。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、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、中新网络信息安全股份有限公司、北京国舜科技股份有限公司、南京联成科技发展股份有限公司、北京智游网安科技有限公司、四川虹微技术有限公司（子午攻防实验室）、山石网科通信技术有限公司、北京明朝万达科技股份有限公司（安元实验室）、河北盾安科技有限公司、河南信安世纪科技有限公司、普华永道商务咨询（上海）有限公司广州分公司及其他个人白帽子向 CNVD 提交了 1261 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 806 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） | 446 | 446 |
| 漏洞盒子 | 360 | 360 |
| 哈尔滨安天科技股份有限公司 | 267 | 0 |
| 蓝盾信息安全技术有限公司 | 200 | 0 |
| 新华三技术有限公司 | 176 | 0 |
| 北京天融信网络安全技术有限公司 | 171 | 12 |
| 华为技术有限公司 | 94 | 0 |
| 北京数字观星科技有限公司 | 57 | 0 |
| 恒安嘉新(北京)科技股份公司 | 56 | 0 |
| 北京神州绿盟科技有限公司 | 52 | 0 |
| 中国电信集团系统集成有限责任公司 | 42 | 0 |
| 北京知道创宇信息技术有限公司 | 41 | 39 |
| 北京无声信息技术有限公司 | 26 | 22 |
| 深圳市深信服电子科技有限公司 | 13 | 0 |
| 沈阳东软系统集成工程有限公司 | 4 | 4 |
| 北京启明星辰信息安全技术有限公司 | 3 | 3 |
| 西安四叶草信息技术有限公司 | 1 | 1 |
| 北京圣博润高新技术股份有限公司 | 50 | 50 |
| 任子行网络技术股份有限公司 | 38 | 38 |
| 山东云天安全技术有限公司 | 35 | 35 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 13 | 13 |

| | | |
|---|---|---|
| 中新网络信息安全股份有限公司 | 11 | 11 |
| 北京国舜科技股份有限公司 | 7 | 7 |
| 南京联成科技发展股份有限公司 | 6 | 6 |
| 北京智游网安科技有限公司 | 3 | 3 |
| 四川虹微技术有限公司（子午攻防实验室） | 2 | 2 |
| 山石网科通信技术有限公司 | 1 | 1 |
| 北京明朝万达科技股份有限公司（安元实验室） | 1 | 1 |
| 河北盾安科技有限公司 | 1 | 1 |
| 河南信安世纪科技有限公司 | 1 | 1 |
| 普华永道商务咨询（上海）有限公司广州分公司 | 1 | 1 |
| CNCERT 山西分中心 | 24 | 24 |
| CNCERT 上海分中心 | 14 | 14 |
| CNCERT 北京分中心 | 9 | 9 |
| CNCERT 黑龙江分中心 | 7 | 7 |
| CNCERT 重庆分中心 | 6 | 6 |
| CNCERT 湖南分中心 | 5 | 5 |
| CNCERT 四川分中心 | 5 | 5 |
| CNCERT 贵州分中心 | 4 | 4 |
| CNCERT 浙江分中心 | 4 | 4 |
| CNCERT 甘肃分中心 | 3 | 3 |
| CNCERT 陕西分中心 | 3 | 3 |
| CNCERT 新疆分中心 | 2 | 2 |
| CNCERT 吉林分中心 | 1 | 1 |

| | | |
|---|---|---|
| CNCERT 天津分中心 | 1 | 1 |
| CNCERT 广东分中心 | 1 | 1 |
| 个人 | 115 | 115 |
| 报送总计 | 2383 | 1261 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 375 个漏洞。应用程序漏洞 106 个，WEB 应用漏洞 87 个，网络设备漏洞 44 个，操作系统漏洞 16 个，安全产品漏洞 12 个，数据库漏洞 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 | 106 |
| WEB 应用漏洞 | 87 |
| 网络设备漏洞 | 44 |
| 操作系统漏洞 | 16 |
| 安全产品漏洞 | 12 |
| 数据库漏洞 | 2 |

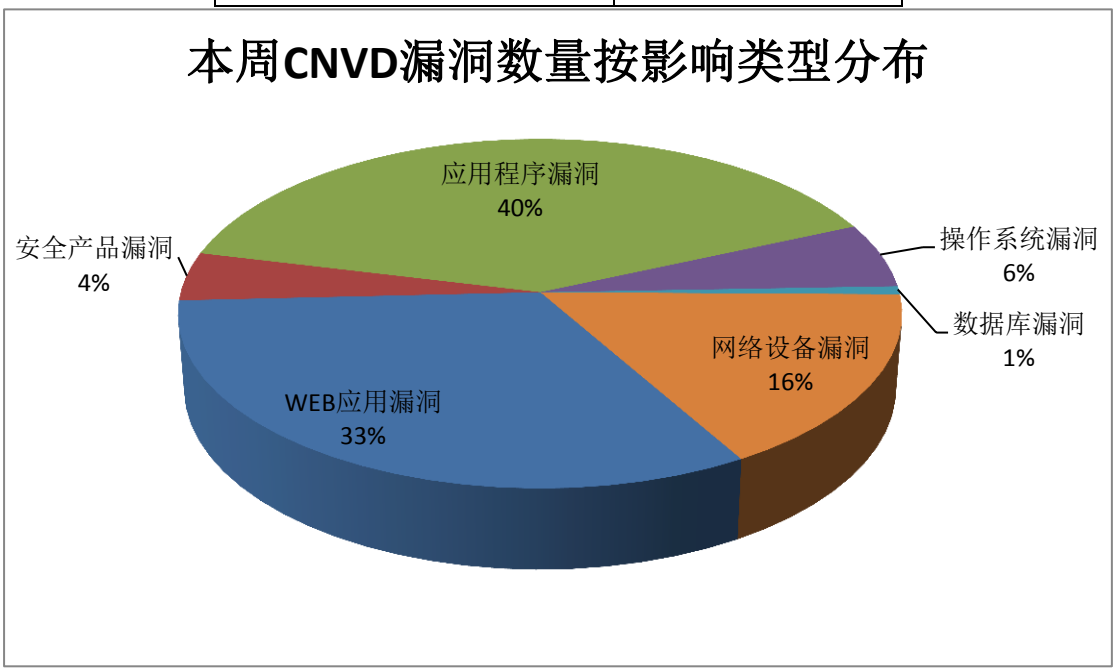


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Joomla!、Samsung、IBM 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 | Joomla! | 17 | 7% |
| 2 | Samsung | 16 | 6% |
| 3 | IBM | 15 | 6% |
| 4 | Cisco | 14 | 5% |
| 5 | Apple | 14 | 5% |
| 6 | Google | 11 | 4% |
| 7 | ZZCMS | 9 | 3% |
| 8 | Ricoh | 8 | 3% |
| 9 | Adobe | 7 | 3% |
| 10 | 其他 | 156 | 58% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 15 个电信行业漏洞，28 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Samsung Galaxy S8 任意代码执行漏洞、Cisco IOS Software Precision Time Protocol 拒绝服务漏洞、Apple iOS Core Bluetooth 组件内存破坏漏洞、Cisco Catalyst 3650 和 3850 Series Switches IOS XE Software 拒绝服务漏洞、Fuji Electric V-Server VPR 内存错误引用漏洞”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/

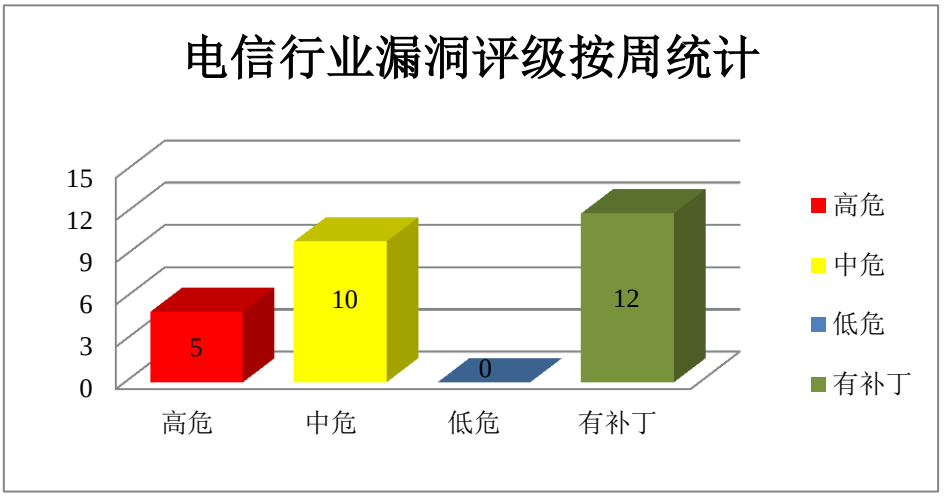


图 3 电信行业漏洞统计

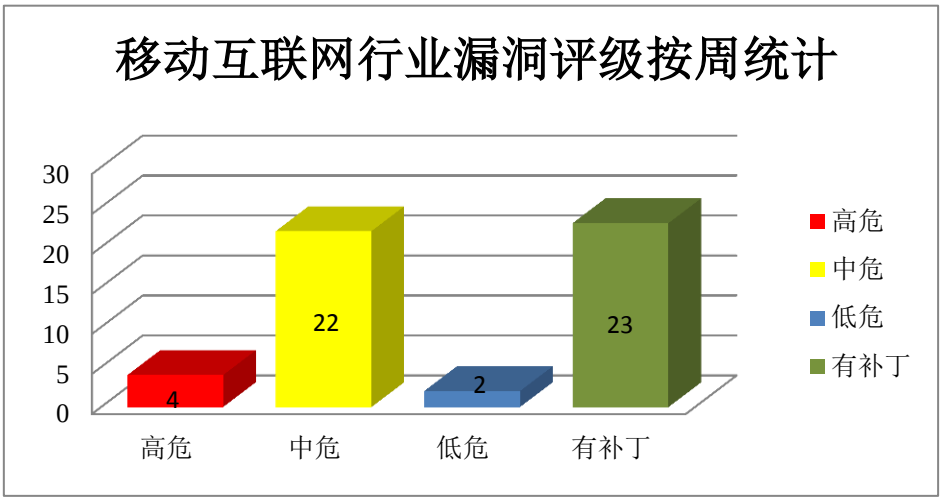


图 4 移动互联网行业漏洞统计

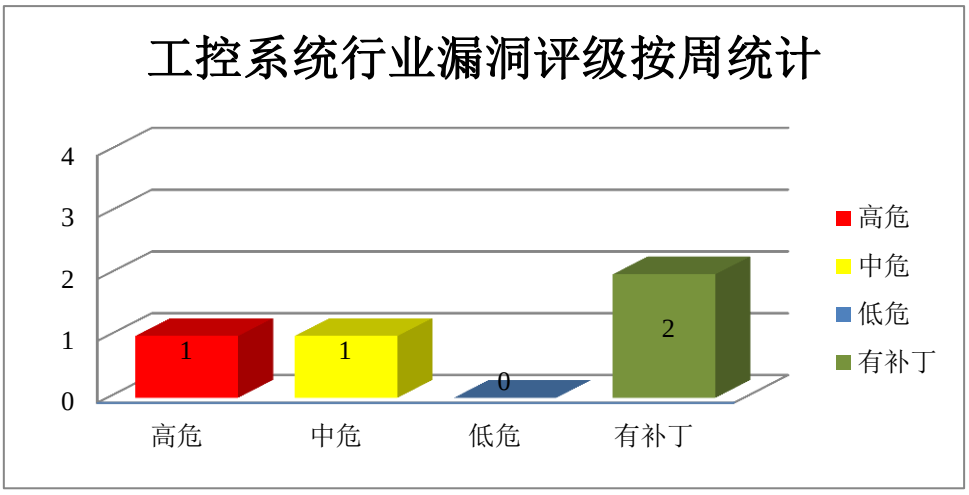


图 5 工控系统行业漏洞统计

## 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、Samsung 产品安全漏洞

Samsung SmartThings Hub STH-ETH-250 是一款智能家居管理设备。本周，上述产品被披露存在缓冲区溢出和任意代码执行漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Samsung SmartThings Hub STH-ETH-250 video-core HTTP 服务器缓冲区溢出漏洞（CNVD-2018-19739、CNVD-2018-19870、CNVD-2018-20124、CNVD-2018-20129、CNVD-2018-20131、CNVD-2018-20132）、Samsung Galaxy S8 任意代码执行漏洞、Samsung SmartThings Hub video-core HTTP 服务器缓冲区溢出漏洞（CNVD-2018-20130）。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-2018-19739

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19870

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20124

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20129

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20131

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20132

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20100

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20130

**2、IBM 产品安全漏洞**

IBM Business Process Manager（BPM）是一套综合的业务流程管理平台。IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。IBM DB2 是一套关系型数据库管理系统。IBM WebSphere Application Server（WAS）是一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。IBM DataPower Gateways 是的一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B 和云工作负载而设计的安全和集成平台，它可利用专用网关平台跨渠道保护、集成和优化访问。IBM Rational Engineering Lifecycle Manager 是一套工程生命周期管理软件。IBM Jazz Foundation 是其中的一套可扩展的团队协作平台。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：IBM Business Process Manager SQL 注入漏洞、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2018-19738）、IBM DB2 缓冲区溢出漏洞（CNVD-2018-20058）、IBM DB2 权限提升漏洞（CNVD-2018-20056）、IBM WebSphere Application Server Liberty 信息泄露漏洞（CNVD-2018-20082）、IBM DataPower Gateway XML 外部实体注入漏洞、IBM DataPower Gateway 信息泄露漏洞、IBM Jazz Foundation XML 外部实体注入漏洞。其中，除“IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2018-19738）、IBM WebSphere Application Server Liberty 信息泄露漏洞（CNVD-2018-20082）、IBM DataPower Gateway 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-2018-19737

http://www.cnvd.org.cn/flaw/show/CNVD-2018-19738

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20058

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20056

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20082

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20104

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20106

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20107

### 3、Cisco 产品安全漏洞

Cisco IOS Software 和 IOS XE Software 都是一套为其网络设备开发的操作系统。Cisco ASA 5500-X Series Adaptive Security Appliance IPsec 是 Cisco 公司安全设备。Cisco Catalyst 3650 和 3850 Series Switches 都是交换机产品。Cisco Second Generation Integrated Services Routers（ISR G2）和 4451-X Integrated Services Router（ISR4451-X）都是路由器产品。Cisco 2500 Series Connected Grid Switches 是交换机产品。本周，上述产品被披露存在拒绝服务和命令注入漏洞，攻击者可利用漏洞以 root 权限在底层 Linux shell 上执行命令，造成拒绝服务。

CNVD 收录的相关漏洞包括：Cisco IOS XE Software 和 Cisco ASA 5500-X Series Adaptive Security Appliance IPsec 拒绝服务漏洞、Cisco IOS XE Software 拒绝服务漏洞（CNVD-2018-20256）、Cisco Catalyst 3650 和 3850 Series Switches IOS XE Software 拒绝服务漏洞、Cisco Second Generation Integrated Services Routers 和 4451-X Integrated Services Router 拒绝服务漏洞、Cisco IOS XE Software NAT SIP ALG 拒绝服务漏洞、Cisco IOS Software Precision Time Protocol 拒绝服务漏洞、Cisco IOS 和 IOS XE Software IPv6 Hop-by-Hop Options 拒绝服务漏洞、Cisco IOS XE Software CLI 解析器命令注入漏洞（CNVD-2018-20300）。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-2018-20048

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20256

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20257

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20258

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20259

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20260

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20261

http://www.cnvd.org.cn/flaw/show/CNVD-2018-20300

### 4、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。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。本周，该产品被披露存在信息泄露和内存破坏漏洞，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：Apple macOS Mojave 信息泄露漏洞、Apple iOS St

atus Bar 组件信息泄露漏洞、Apple iOS Core Bluetooth 组件内存破坏漏洞、Apple iOS CoreMedia 组件信息泄露漏洞、Apple iOS IOMobileFrameBuffer 组件信息泄露漏洞、Apple iOS Accounts 组件信息泄露漏洞、Apple iOS 和 tvOS Kernel 信息泄露漏洞、Apple iOS 和 tvOS Messages 和 Safari 信息泄露漏洞。其中，“Apple iOS Core Bluetooth 组件内存破坏漏洞”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-2018-20105
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20203
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20204
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20205
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20206
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20210
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20208
http://www.cnvd.org.cn/flaw/show/CNVD-2018-20209

**5、MODX Revolution 跨站脚本漏洞（CNVD-2018-20075）**

MODX Revolution 是美国 MODX 公司的一套基于 PHP 的开源内容管理系统（CMS）。该系统支持在线协作、搜索引擎优化（SEO）、附加组件等。本周，MODX Revolution 被披露存在跨站脚本漏洞。远程攻击者可通过选择 Create New Media Source 利用该漏洞将 HTML 标签或脚本存储在数据库中。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-2018-20075

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-2018-19667 | Antidote 远程代码执行漏洞 | 高 | 用户可联系供应商获得补丁信息：https://www.antidote.info/ |
| CNVD-2018-19731 | ThinkLC 后台存在命令执行漏洞 | 高 | 厂商尚未提供漏洞修复方案，请关注厂商主页更新：http://www.saxue.com/ |
| CNVD-2018-19740 | Tec4Data SmartCooler 拒绝服务漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：http://www.tec4data.com/ |
| CNVD-2018-19746 | Joomla! CWJoomla CW Article Attachments 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：http://www.cwjoomla.com/ |
| CNVD-2018-19867 | Slack ArchiveBot SQL 注入漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新： |

| | | | |
|---|---|---|---|
| | | | https://github.com/docmarionum1/slack-archive-bot/pull/13/files |
| CNVD-2018-19929 | Linux kernel create_elf_tables()整数溢出漏洞 | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://access.redhat.com/errata/RHSA-2018:2763 |
| CNVD-2018-20087 | Dell EMC RSA Authentication Manager Operations Console 跨站脚本漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/ |
| CNVD-2018-20133 | Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2018-20133） | 高 | 厂商已发布漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb18-34.html |
| CNVD-2018-20139 | Google Chrome V8 International Components for Unicode 整数溢出漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://chromereleases.googleblog.com/2017/12/stable-channel-update-for-desktop.html |
| CNVD-2018-20216 | HPE Integrated Lights-Out 5 任意代码执行漏洞 | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03866en_us |

小结：本周，Samsung 被披露存在缓冲区溢出和任意代码执行漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。此外，IBM、Cisco、Apple 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），造成拒绝服务等。另外，MODX Revolution 被披露存在跨站脚本漏洞。远程攻击者可通过选择 Create New Media Source 利用该漏洞将 HTML 标签或脚本存储在数据库中。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、LG SuperSign CMS 远程代码执行漏洞

**验证描述**

LG SuperSign CMS 是韩国乐金（LG）集团的一套针对 LG webOS 的内容管理系统。该系统支持连接外部数据库，并允许从移动设备访问服务器。

LG SuperSign CMS 中存在远程代码执行漏洞，远程攻击可通过向 qsr_server/device/getThumbnail 发送‘sourceUri’参数利用该漏洞执行任意代码。

**验证信息**

POC 链接：https://www.exploit-db.com/exploits/45448/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-19935

**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. Linux 爆出严重内核漏洞，可为攻击者提供 Root 访问权限

所有版本的 Red Hat Enterprise Linux 和 CentOS 都容易受到该整数溢出漏洞（CVE-2018-14634）的影响。它为攻击者提供了一种获取系统完整 root 访问权限的方法。整数溢出漏洞（CVE-2018-14634）存在于用于内存管理的关键 Linux 内核函数 create_elf_tables（）中。在 64 位系统上，本地攻击者可以通过 SUID root 二进制文件利用此漏洞并获取完整的 root 特权。

参考链接：https://www.darkreading.com/vulnerabilities---threats/critical-linux-kernel-flaw-gives-root-access-to-attackers/d/d-id/1332906?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple

### 2. 80 多款思科产品受到 FragmentSmack DOS 漏洞影响

近期，思科正在审查产品线，因为其使用 Linux 内核 3.9 及以上的产品和服务受到 FragmentSmack DOS 漏洞影响，需要进行安全修复。目前，思科共列出了 80 多款受影响的产品。其中大部分要到 2019 年 2 月份才能修复。这些产品主要是企业和服务供应商专用的路由和交换机类产品（APIC-EM）。目前，由于尚未发布补丁，思科建议用户检查产品特定文档，寻求可能的解决方案。

参考链接：https://www.bleepingcomputer.com/news/security/over-80-cisco-products-affected-by-fragmentsmack-dos-bug/?tdsourcetag=s_pctim_aiomsg

### 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