国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 6 月 25 日-2018 年 7 月 1 日 **2018 年第 26 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 285 个，其中高危漏洞 107 个、中危漏洞 168 个、低危漏洞 10 个。漏洞平均分值为 6.25。本周收录的漏洞中，涉及 0day 漏洞 54 个（占 19%），其中互联网上出现“TP-Link TL-WR841N v13 认证命令注入漏洞、Joomla! com_regionalm Icta Regional Museum 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 393 个，与上周（476 个）环比下降 17%。

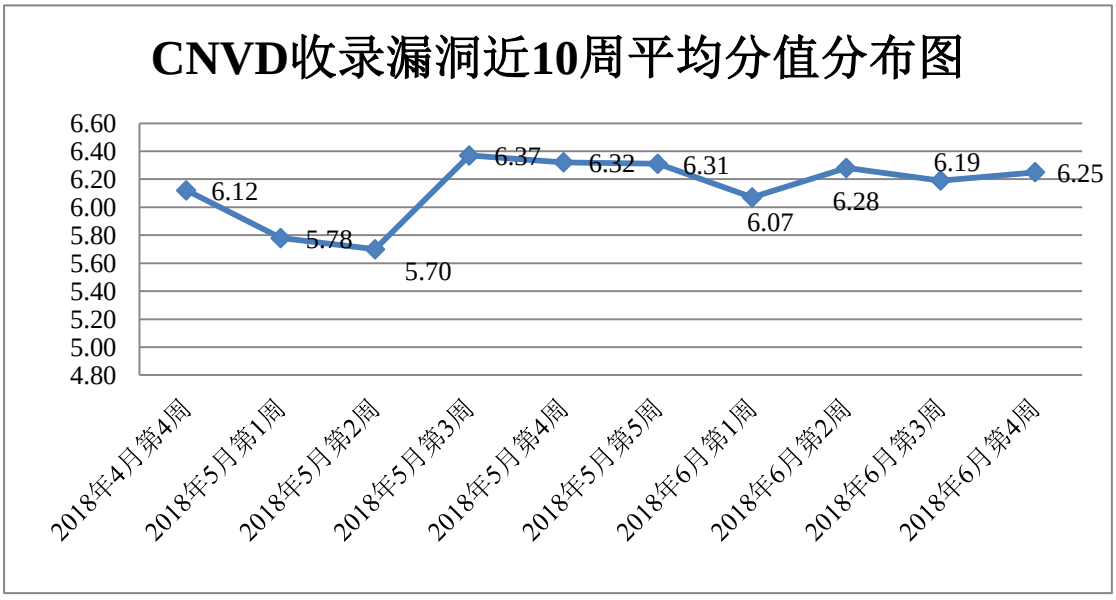

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 13 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 180 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 247 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：

博控电气有限公司、深圳市航力晟科技有限公司、大唐财富投资管理有限公司、南软科技发展有限公司、临沂市新网网络科技有限公司、北京沃丰时代数据科技有限公司、海南赞赞网络科技有限公司、上海思顶信息科技有限公司、深圳市英威腾电气股份有限公司、苏州科达科技股份有限公司、洪湖尔创网联信息技术有限公司、北京极科极客科技有限公司、国通集团、中国工控 ABB 中国客户服务中心、BEESCMS、中国医药保健品进出口商会、中国红十字会、生态养老产业委员会、财新网。

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、杭州安恒信息技术有限公司、哈尔滨安天科技股份有限公司、华为技术有限公司、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。四川虹微技术有限公司（子午攻防实验室）、北京国舜科技股份有限公司、上海纽盾科技股份有限公司、济南三泽信息安全测评有限公司、河南信安世纪科技有限公司、山东云天安全技术有限公司、北京明朝万达科技股份有限公司（安元实验室）、任子行网络技术股份有限公司、安徽锋刃信息科技有限公司、北京智游网安科技有限公司、山石网科通信技术有限公司、成都思维世纪科技有限公司、江苏省信息安全测评中心、福建六壬网安股份有限公司及其他个人白帽子向 CNVD 提交了 393 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 194 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
北京天融信网络安全技术有限公司	271	1
杭州安恒信息技术有限公司	245	0
哈尔滨安天科技股份有限公司	218	0
华为技术有限公司	174	0
360 网神（补天平台）	118	118

漏洞盒子	76	76
北京神州绿盟科技有限公司	75	1
中国电信集团系统集成有限责任公司	68	0
新华三技术有限公司	63	0
北京数字观星科技有限公司	50	0
北京无声信息技术有限公司	21	0
厦门服云信息科技有限公司	19	0
恒安嘉新(北京)科技股份公司	11	11
北京知道创宇信息技术有限公司	2	1
南京联成科技发展股份有限公司	13	13
中新网络信息安全股份有限公司	13	13
四川虹微技术有限公司（子午攻防实验室）	5	5
北京国舜科技股份有限公司	5	5
上海纽盾科技股份有限公司	4	4
济南三泽信息安全测评有限公司	4	4
河南信安世纪科技有限公司	2	2
山东云天安全技术有限公司	2	2
北京明朝万达科技股份有限公司（安元实验室）	2	2
任子行网络技术股份有限公司	2	2
安徽锋刃信息科技有限公司	1	1
北京智游网安科技有限公司	1	1
山石网科通信技术有限公司	1	1

成都思维世纪科技有限公司	1	1
江苏省信息安全测评中心	1	1
福建六壬网安股份有限公司	1	1
CNCERT 上海分中心	16	16
CNCERT 陕西分中心	13	13
CNCERT 宁夏分中心	7	7
CNCERT 湖南分中心	6	6
CNCERT 海南分中心	5	5
CNCERT 天津分中心	4	4
CNCERT 甘肃分中心	2	2
CNCERT 新疆分中心	1	1
个人	73	73
报送总计	1596	393

本周漏洞按类型和厂商统计

本周，CNVD 收录了 285 个漏洞。其中应用程序漏洞 136 个，操作系统漏洞 52 个，WEB 应用漏洞 48 个，网络设备漏洞 43 个，安全产品漏洞 6 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	136
操作系统漏洞	52
WEB 应用漏洞	48
网络设备漏洞	43
安全产品漏洞	6

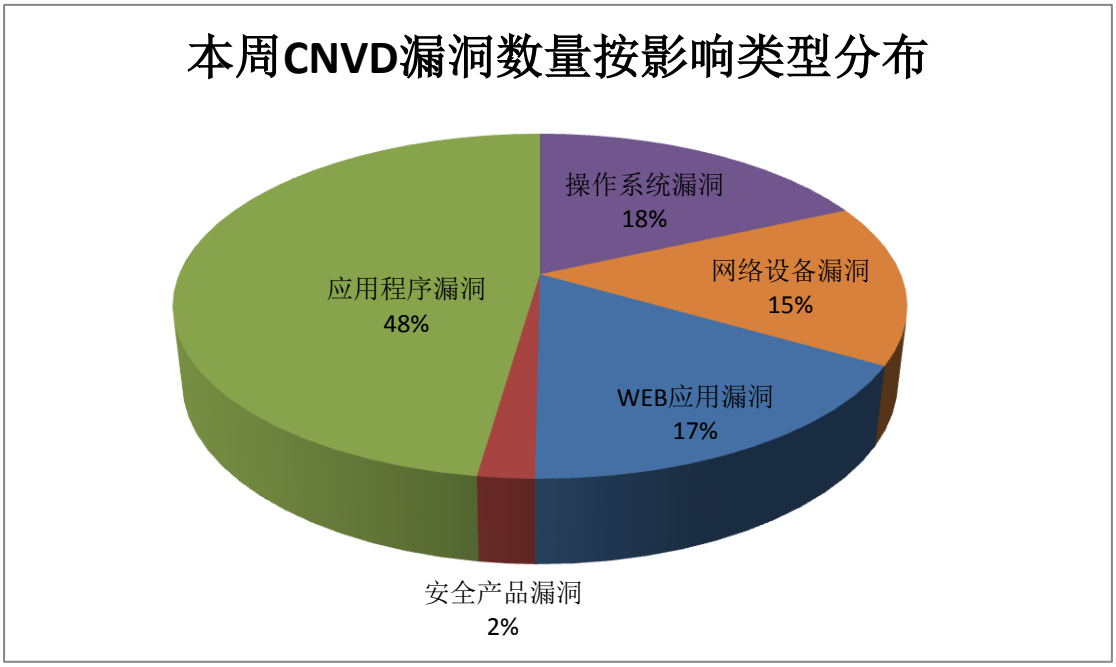

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Cisco、ImageMagick 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	Apple	43	15%
2	Cisco	15	5%
3	Radare	12	4%
4	ImageMagick	11	4%
5	Google	11	4%
6	Mozilla	11	4%
7	Wireshark	9	3%
8	SLiMS 8	6	2%
9	Natus Medical	5	2%
10	其他	162	57%

本周行业漏洞收录情况

本周，CNVD 收录了 23 个电信行业漏洞，47 个移动互联网行业漏洞，26 个工控行业漏洞（如下图所示）。其中，“Rockwell Automation RSLinx Classic and FactoryTalk Linx Gateway 权限提升漏洞、Delta Industrial Automation DOPSoft 越界读取漏洞、多款 Apple

产品 WebKit 类型混淆漏洞、TP-Link TL-WR841N v13 身份验证漏洞、多款 Cisco 产品 NX-OS Software SNMP 拒绝服务漏洞”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/

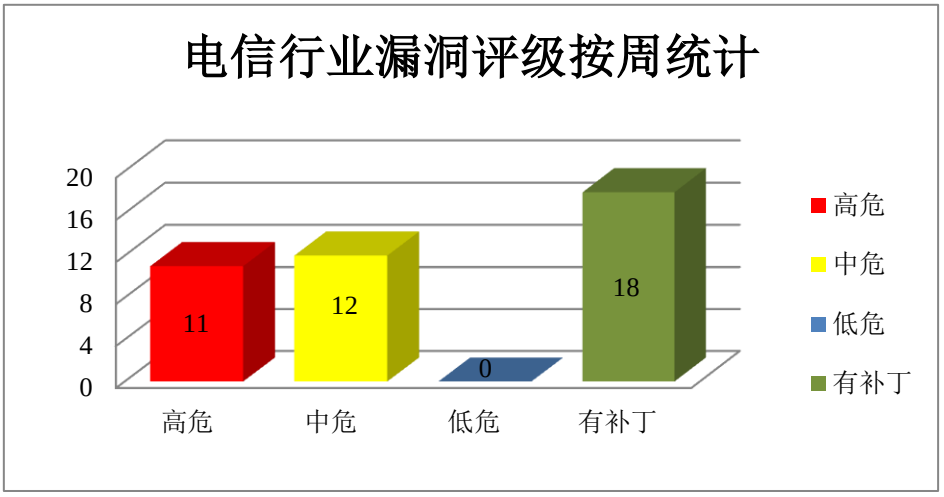

图 3 电信行业漏洞统计

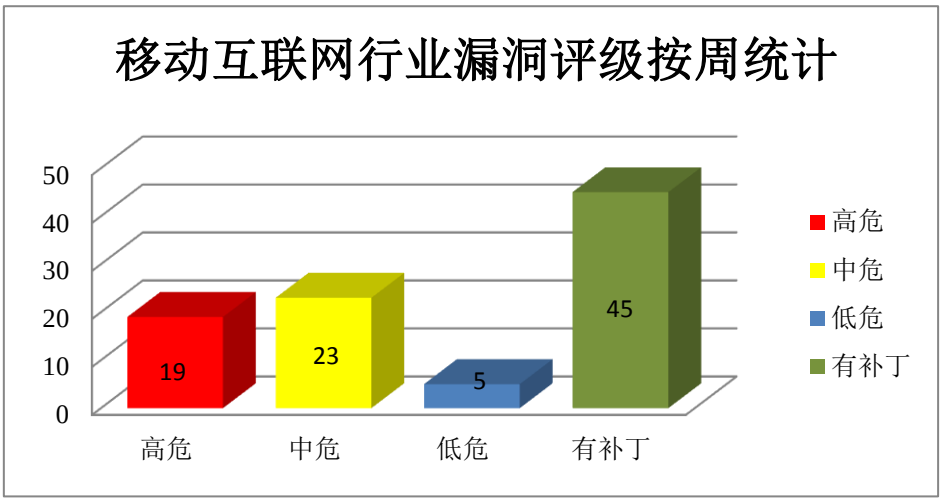

图 4 移动互联网行业漏洞统计

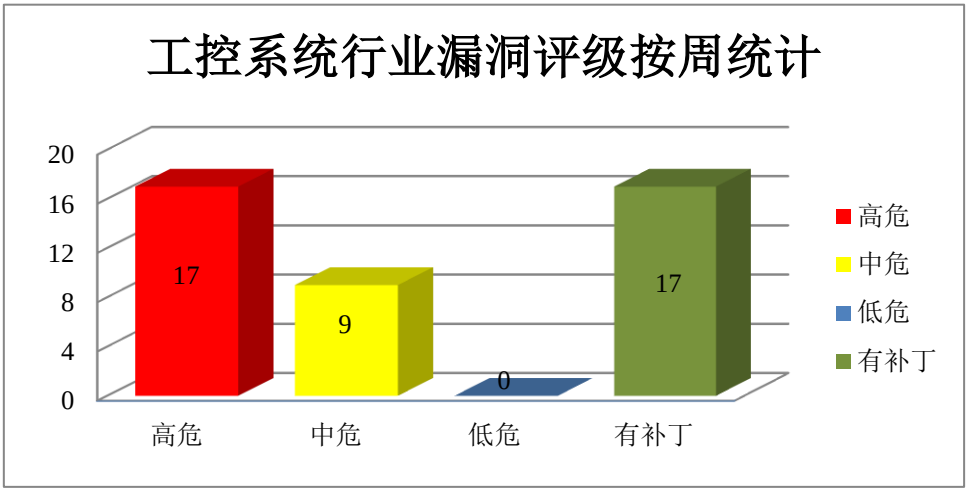

图 5 工控系统行业漏洞统计

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、Apple 产品安全漏洞

Apple macOS High Sierra 是为 Mac 计算机所开发的一套专用操作系统。Apple iOS 是为移动设备所开发的一套操作系统；macOS High Sierra 是一套专为 Mac 计算机所开发的专用操作系统；tvOS 是一套智能电视操作系统；watchOS 是一套智能手表操作系统。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发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple macOS High Sierra 任意代码执行漏洞（CNVD-2018-12162）、Apple macOS High Sierra 内存破坏漏洞（CNVD-2018-12163、CNVD-2018-12164、CNVD-2018-12245）、多款 apple 产品拒绝服务漏洞（CNVD-2018-12165、CNVD-2018-12193、CNVD-2018-12194）、Apple macOS High Sierra NVIDIA Graphics 驱动程序任意代码执行漏洞。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-2018-12162

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12163

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12164

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12245

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12165

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12193

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12194

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12255

2、Cisco 产品安全漏洞

Cisco NX-OS Software 是一套面向数据中心的操作系统。Cisco Acano X-Series、Meeting Server 1000 和 Meeting Server 2000 都是视频会议解决方案。Cisco Nexus 2000 Series Switches 是交换机设备。Cisco Firepower 4100 Series Next-Generation Firewalls 是一款 4100 系列的防火墙设备。MDS 9000 Series Multilayer Switches 是一款交换机设备。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，执行远程代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco NX-OS 任意命令执行漏洞、Cisco Meeting Server Web 管理界面拒绝服务漏洞、多款 Cisco 产品 NX-OS Software 拒绝服务漏洞、多款 Cisco 产品 NX-OS Software NX-API management API 权限提升漏洞、多款 Cisco 产品 NX-OS Software 缓冲区溢出漏洞、多款 Cisco 产品 NX-OS Software 任意命令执行漏洞、多款 Cisco 产品 NX-OS Software SNMP 拒绝服务漏洞、多款 Cisco 产品拒绝服务漏洞（CNVD-2018-12392）。其中，除“Cisco NX-OS 任意命令执行漏洞”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-2018-11973

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12112

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12386

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12389

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12390

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12391

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12393

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12392

3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 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，攻击者可利用漏洞获取敏感信息，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：Google Chrome Media Cache 内存错误引用漏洞、Google Android WLAN 缓冲区溢出漏洞（CNVD-2018-12402、CNVD-2018-12403）、Google Android System 远程代码执行漏洞（CNVD-2018-12404、CNVD-2018-12406、CNVD-2018-12405）、Google Android System 信息泄露漏洞（CNVD-2018-12407、CNVD-2018-12408）。其中，“Google Chrome Media Cache 内存错误引用漏洞、Google Android System 远程代码执行漏洞（CNVD-2018-12404、CNVD-2018-12406、CNVD-2018-12405）”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-2018-11996

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12402

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12403

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12404

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12406

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12405

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12407

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12408

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。Thunderbird 是从 Mozilla Application Suite 中独立出来的一套电子邮件客户端软件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞破坏内存，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：Mozilla Firefox、Firefox ESR 和 Thunderbird 内存破坏漏洞（CNVD-2018-12100）、Mozilla Firefox Skia 内存破坏漏洞、Mozilla Firefox、Firefox ESR 和 Thunderbird 内存破坏漏洞（CNVD-2018-12102）、Mozilla Firefox 内存破坏漏洞（CNVD-2018-12101）、Mozilla Firefox 和 Firefox ESR 内存错误引用漏洞（CNVD-2018-12395）、Mozilla Firefox 和 Firefox ESR 整数溢出漏洞（CNVD-2018-12396）、Mozilla Firefox 和 Firefox 整数溢出漏洞（CNVD-2018-12397）、Mozilla Firefox 和 Firefox ESR 双重释放漏洞。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-2018-12100

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12099

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12102

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12101

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12395

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12396

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12397

http://www.cnvd.org.cn/flaw/show/CNVD-2018-12398

5、AsusWRT RT-AC750GF 跨站请求伪造漏洞

RT-AC750GF 是 ASUS 公司路由器产品。本周，AsusWRT RT-AC750GF 被披露存在跨站请求伪造漏洞，攻击者可利用漏洞更改管理员密码。目前，厂商尚未发布漏洞修补程序。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-2018-12126

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-2018-11989	TIBCO Data Virtualization 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.tibco.com/support/advisories/2018/06/tibco-security-advisory-june-20-2018-tibco-data-virtualization
CNVD-2018-11991	ABB IP Gateway 未授权访问漏洞（CNVD-2018-11991）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://new.abb.com/about/technology/cyber-security/alerts-and-notifications
CNVD-2018-12042	Microsoft SharePoint Server 权限提升漏洞（CNVD-2018-12042）	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/en-US/security-guidance/advisory/CVE-2018-8254
CNVD-2018-12105	Cloud Foundry Diego 权限获取漏洞	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.cloudfoundry.org/blog/cve-2018-1265/
CNVD-2018-12116	iThemes Security 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://wordpress.org/plugins/better-wp-security/#developers
CNVD-2018-12127	多款 Rockwell Automation 产品输入验证漏洞	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.rockwellautomation.com
CNVD-2018-12128	Delta Electronics Delta Industrial Automation COMMGR 缓冲区溢出漏洞	高	目前供应商发布了安全公告及相关补丁信息，修复了此漏洞：http://www.deltaww.com/Products/PluginWebUserControl/downloadCenterCounter.aspx?DID=2093&DocPath=1&hl=en-USl
CNVD-2018-12147	Micro Focus SUSE Linux Enterprise sysconfig 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://www.suse.com/security/cve/CVE-2017-15710/
CNVD-2018-12151	McAfee Network Security Management 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kc.mcafee.com/corporate/index?

			page=content&id=SB10192
CNVD-2018-12154	Linux kernel 内存破坏漏洞（CNVD-2018-12154）	高	用户可联系供应商获得补丁信息：https://www.kernel.org/

小结：本周，Apple 被披露存在多个漏洞，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，Cisco、Google、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，破坏内存，提升权限，执行远程代码或发起拒绝服务攻击。另外，AsusWRT RT-AC750GF 被披露存在跨站请求伪造漏洞，攻击者可利用漏洞更改管理员密码。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、TP-Link TL-WR841N v13 认证命令注入漏洞

验证描述

TP-Link TL-WR841N v13 是一款无线路由器设备。

TP-Link TL-WR841N v13 ping 和 traceroute 功能存在认证命令注入漏洞。经过身份验证的攻击者可以通过向路由器发送特定的 CREST HTTP 请求在路由器上执行任意命令。

验证信息

POC 链接：http://seclists.org/bugtraq/2018/Jun/66

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-12337

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. 自 2012 年以来，所有 Android 设备都受到 RAMpage 漏洞的影响

新的 RAMpage 漏洞是 Rowhammer 攻击的一个变种。RAMpage 可以破坏用户 app 和操作系统的隔离。一般来说一款应用不能获取其他应用的数据，但利用 RAMpage 漏洞，攻击者可以获得管理员权限，获取设备中的机密信息。机密信息可能包括密码管理器或者浏览器中存储的密码，你的个人照片、邮件、即时消息或者是工作文件。对 RAMpage 的研究还停留在早期阶段，然研究人员称，RAMpage 也可以被用来攻击苹果、PC 设备以及虚拟机。

参考链接：https://www.bleepingcomputer.com/news/security/every-android-device-since-2012-impacted-by-rampage-vulnerability/

2. Fredi 的无线婴儿监控存在漏洞可被利用为间谍摄像机

近日，安全研究人员发布报告称，Fredi 公司的无线婴儿监控设备存在严重漏洞，该漏洞可被未经身份验证的攻击者所利用，不仅能够监控他人还能藉此入侵整个家庭网络。研究人员表示，很多商用的监控设备都会默认开启 P2P 云功能，在使用过程中将其连接到云服务架构中并保持连接状态。用户可以通过移动设备以及桌面应用程序通过云端访问其设备。

参考链接：http://www.freebuf.com/news/175820.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