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 04 日-2019 年 03 月 10 日 **2019 年第 10 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 240 个，其中高危漏洞 105 个、中危漏洞 122 个、低危漏洞 13 个。漏洞平均分值为 6.38。本周收录的漏洞中，涉及 0day 漏洞 115 个（占 48%），其中互联网上出现“FiberHome Fiberhome AN5506-04-F 跨站脚本漏洞、OFCMS 后台 ueditor uploadScrawl 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 1916 个，与上周（1944 个）环比下降 1%。

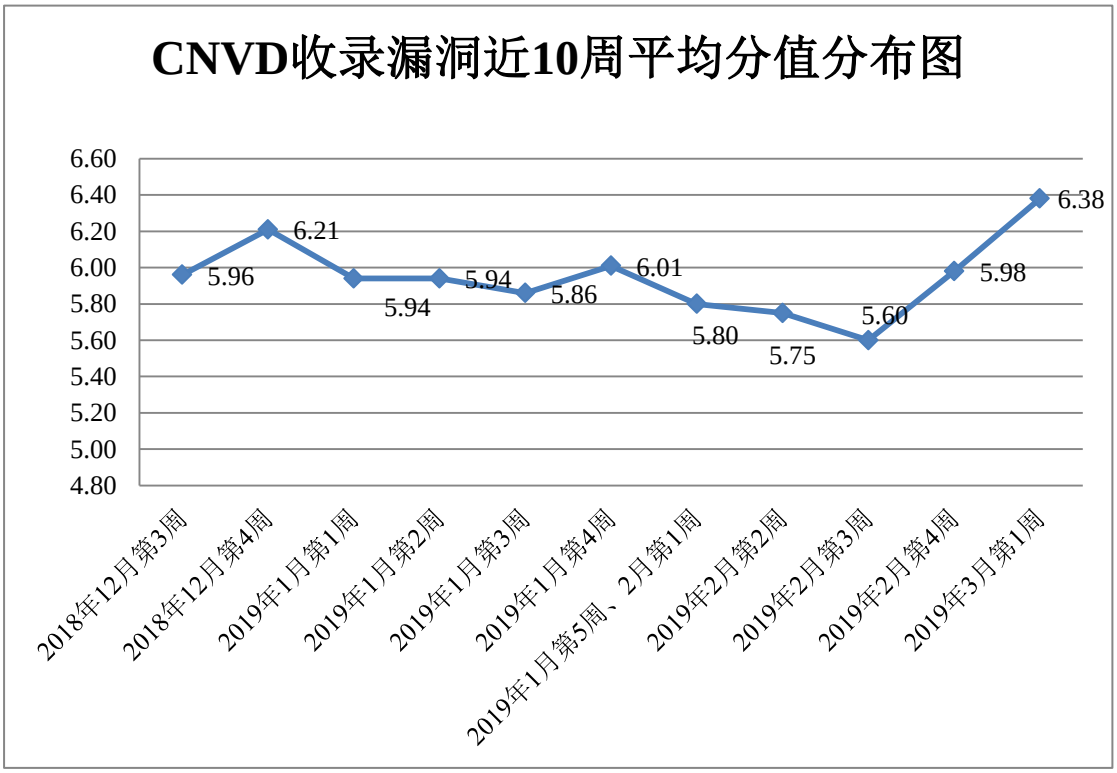

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 39 起，向银行、保险、能源等重要行业单位通报漏洞事件 29 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 1265 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 106 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 33 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：

爱瑞思软件（深圳）有限公司、微软(中国)有限公司、上海馨澈实业有限公司、厦门创云科技有限公司、长春市支点科技有限公司、西安三才科技实业有限公司、福州极限软件开发有限公司、北京亿赛通科技发展有限责任公司、淄博闪灵网络科技有限公司、厦门云脉技术有限公司、漳州豆壳网络科技有限公司、桂林崇胜网络科技有限公司、天津企航志成科技有限公司、广州齐博网络科技有限公司、重庆然宇网络科技有限公司、墨子科技、新秀工作室、深圳好生意网络工作室、超级 CMS、易贝 CMS、WMCMS 团队、HYBBS、Icms、Odoo、zzzcms。

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、四川无声信息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、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、山东华鲁科技发展股份有限公司、北京国舜科技股份有限公司、四川月安客信息技术有限公司、河南信安世纪科技有限公司、山石网科通信技术股份有限公司、北京安信天行科技有限公司、北京长亭科技有限公司、江苏保旺达软件技术有限公司、内蒙古奥创科技有限公司、北京圣博润高新技术股份有限公司、山东九州信泰信息科技股份有限公司及其他个人白帽子向 CNVD 提交了 1916 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 1436 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
斗象科技（漏洞盒子）	865	865
360 网神（补天平台）	571	571
华为技术有限公司	157	0
哈尔滨安天科技集团股份有限公司	156	0

北京天融信网络安全技术有限公司	95	10
新华三技术有限公司	73	0
四川无声信息技术有限公司	56	56
北京启明星辰信息安全技术有限公司	44	2
中国电信集团系统集成有限责任公司	42	0
北京数字观星科技有限公司	39	0
北京神州绿盟科技有限公司	39	0
恒安嘉新(北京)科技股份公司	25	0
厦门服云信息科技有限公司	25	0
深信服科技股份有限公司	15	0
北京知道创宇信息技术有限公司	13	5
国瑞数码零点实验室	80	80
中新网络信息安全股份有限公司	75	75
南京联成科技发展股份有限公司	33	33
山东华鲁科技发展股份有限公司	14	14
北京国舜科技股份有限公司	5	5
四川月安客信息技术有限公司	5	5
河南信安世纪科技有限公司	4	4
山石网科通信技术股份有限公司	3	3
北京安信天行科技有限公司	2	2
北京长亭科技有限公司	2	2
江苏保旺达软件技术有限公司	2	2

内蒙古奥创科技有限公司	2	2
北京圣博润高新技术股份有限公司	1	1
山东九州信泰信息科技股份有限公司	1	1
CNCERT 吉林分中心	10	10
CNCERT 天津分中心	10	10
CNCERT 贵州分中心	4	4
CNCERT 陕西分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	150	150
报送总计	2622	1916

本周漏洞按类型和厂商统计

本周，CNVD 收录了 240 个漏洞。应用程序漏洞 131 个，WEB 应用漏洞 61 个，网络设备漏洞 32 个，操作系统漏洞 15 个，安全产品漏洞 1 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	131
WEB 应用漏洞	61
网络设备漏洞	32
操作系统漏洞	15
安全产品漏洞	1

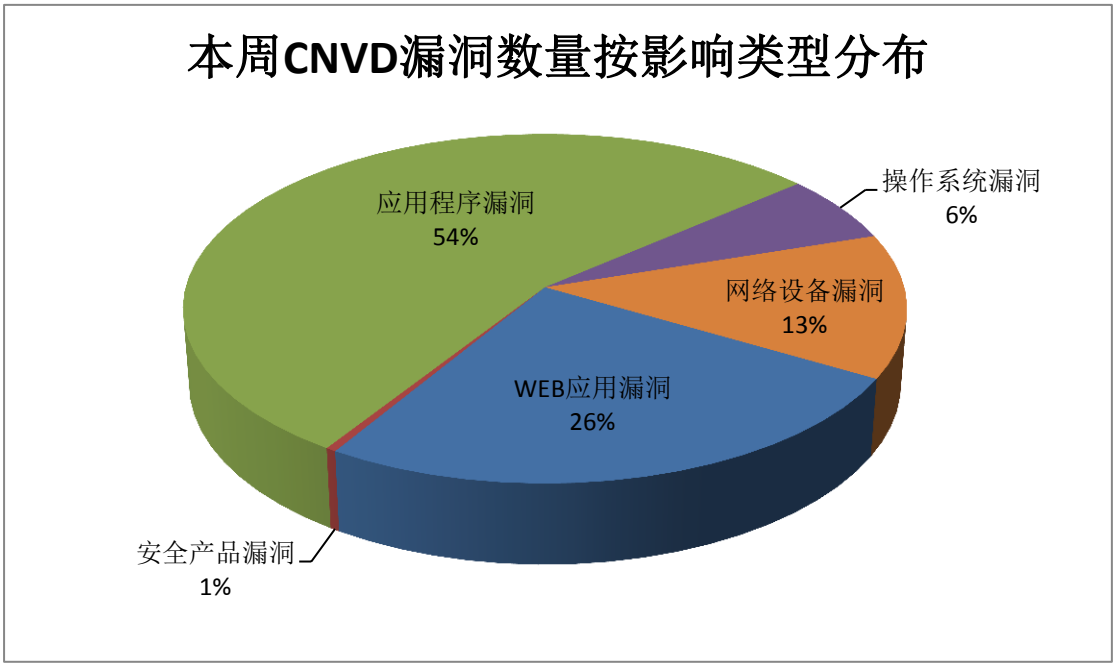

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Linux、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	Cisco	17	7%
2	Linux	11	5%
3	IBM	11	5%
4	Moxa	11	5%
5	OFCMS	10	4%
6	Wireshark	9	3%
7	Google	8	3%
8	ACD Systems	6	3%
9	DASAN Networks	6	3%
10	其他	151	62%

本周行业漏洞收录情况

本周，CNVD 收录了 21 个电信行业漏洞，15 个工控行业漏洞（如下图所示）。其中，“Cisco Nexus 9000 ACI 模式权限提升漏洞、Moxa IKS 和 EDS 跨站请求伪造漏洞、ZTE ZXR10 1800-2S ZSRV2 验证绕过漏洞、Cisco Nexus 9000 系列交换矩阵交换机本地

命令注入漏洞、Moxa IKS 和 EDS 不受控资源消耗漏洞”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/

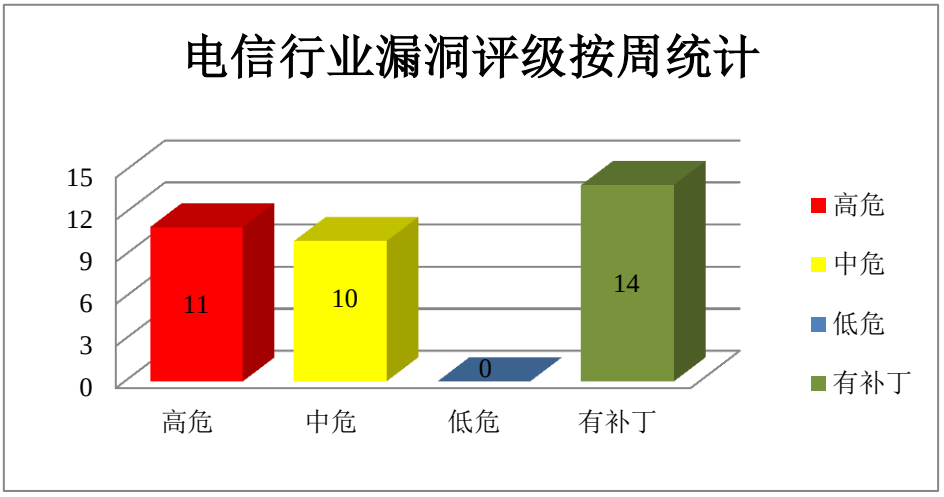

图 3 电信行业漏洞统计

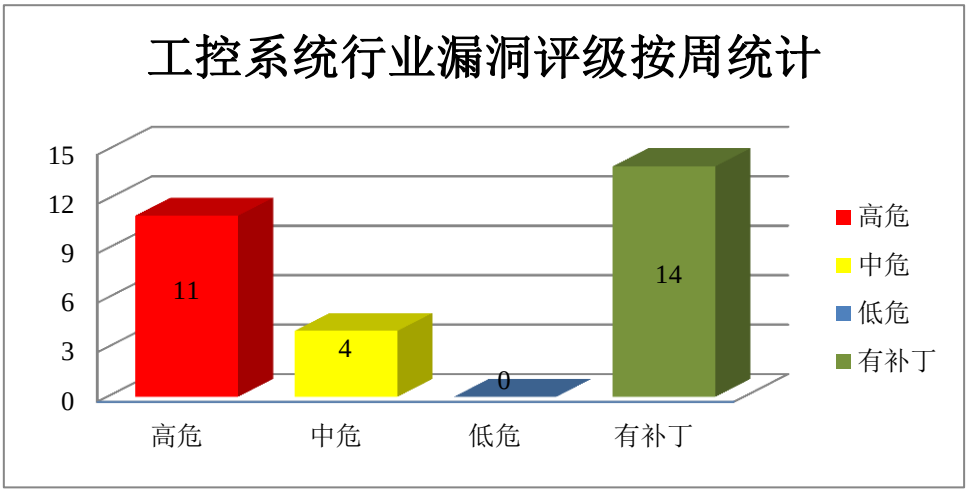

图 4 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco HyperFlex Software 是一套可扩展的分布式文件系统。Cisco Prime Infrastructure 是一种网络管理工具，支持从一个图形界面对整个网络基础设施进行全生命周期管理。Cisco Nexus 9000 系列交换机是专为数据中心设计的模块化和固定端口网络交换机。Cisco NX-OS 是一套交换机使用的数据中心级操作系统软件。本周，上述产

品被披露存在多个漏洞，攻击者可利用漏洞实施中间人攻击，查看并修改敏感信息，提升权限，执行任意命令，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco HyperFlex 跨站脚本漏洞、Cisco HyperFlex Software 远程命令注入漏洞、Cisco Prime Infrastructure SSL 证书验证安全绕过漏洞、Cisco Nexus 9000 ACI 模式任意文件读取漏洞、Cisco Nexus 9000 ACI 模式权限提升漏洞、Cisco NX-OS 拒绝服务漏洞、Cisco NX-OS 权限提升漏洞、Cisco Nexus 9000 系列交换矩阵交换机本地命令注入漏洞。其中，“Cisco HyperFlex Software 远程命令注入漏洞、Cisco Nexus 9000 ACI 模式权限提升漏洞、Cisco NX-OS 权限提升漏洞、Cisco Nexus 9000 系列交换矩阵交换机本地命令注入漏洞”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-2019-06585
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06587
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06588
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06595
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06596
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06604
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06605
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06606

2、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的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多个漏洞，攻击者可利用漏洞提升权限，造成拒绝服务或执行任务代码。

CNVD 收录的相关漏洞包括：Linux kernel 'update_blocked_averages'函数无限循环漏洞、Linux kernel 内存错误引用漏洞（CNVD-2019-06182）、Linux kernel 本地权限提升漏洞（CNVD-2019-06183）、Linux kernel drivers/char/ipmi/ipmi_msghandler.c 文件内存错误引用漏洞、Linux Kernel 'xfs_attr.c'本地拒绝服务漏洞、Linux kernel 'usb_audio_probe'函数内存错误引用漏洞、Linux kernel 子系统拒绝服务漏洞、Linux kernel NFS41+子系统内存错误引用漏洞。其中，“Linux kernel 'update_blocked_averages'函数无限循环漏洞、Linux kernel 内存错误引用漏洞（CNVD-2019-06182）、Linux kernel drivers/char/ipmi/ipmi_msghandler.c 文件内存错误引用漏洞、Linux kernel 子系统拒绝服务漏洞”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-2019-06180
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06182

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06183

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06181

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06577

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06581

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06582

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06583

3、IBM 产品安全漏洞

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 Cloud Private 是一套企业私有云解决方案。IBM Rational DOORS Next Generation（DNG/RRC）是一套用于捕获、跟踪、分析和管理需求的软件。IBM WebSphere Application Server（WAS）是一款应用服务器产品。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 URL，实施钓鱼攻击，获取敏感信息，向 Web UI 中注入任意的 JavaScript 代码。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator 跨站脚本漏洞（CNVD-2019-06044、CNVD-2019-06047、CNVD-2019-06160）、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2019-06050）、IBM Cloud Private 信息泄露漏洞（CNVD-2019-06159）、IBM Cloud Private 重定向漏洞、IBM Rational DOORS Next Generation 跨站脚本漏洞（CNVD-2019-06352）、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2019-06354）。其中，“IBM Cloud Private 重定向漏洞” 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-2019-06044

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06050

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06047

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06159

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06160

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06162

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06352

http://www.cnvd.org.cn/flaw/show/CNVD-2019-06354

4、Moxa 产品安全漏洞

Moxa IKS 和 EDS 是 Moxa 推出的工业交换机系列。Moxa NPort W2x50A 是一款用于将工业串口设备连上网络的串口通讯服务器。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，执行任意代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Moxa IKS 和 EDS 越界读取漏洞、Moxa IKS 和 EDS 明文密码存储漏洞、Moxa IKS 和 EDS 不受控资源消耗漏洞、Moxa NPort W2x50A 操

作系统命令注入漏洞、Moxa IKS 和 EDS 缓冲区溢出漏洞、Moxa IKS 和 EDS 跨站请求伪造漏洞、Moxa IKS 和 EDS 跨站脚本漏洞、Moxa IKS 和 EDS 访问控制不当漏洞。上述漏洞的综合评级为“高危”。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-2019-06056
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06057
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06059
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06176
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06175
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06177
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06178
http://www.cnvd.org.cn/flaw/show/CNVD-2019-06179

5、Dell EMC RSA Archer 信息泄露漏洞（CNVD-2019-06042）

Dell EMC RSA Archer 是一款企业 IT 治理和合规治理产品。本周，Dell EMC RSA Archer 被披露存在信息泄露漏洞。攻击者可利用该漏洞泄露信息。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-2019-06042

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-2019-05943	OpenMRS 反序列命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://openmrs.org/
CNVD-2019-06041	Dell EMC RSA Archer 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dellemc.com/
CNVD-2019-06048	Adobe ColdFusion 任意文件上传漏洞（CNVD-2018-18733）	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://helpx.adobe.com/security/products/coldfusion/apsb19-14.html
CNVD-2019-06164	Wireshark 拒绝服务漏洞（CNVD-2019-06164）	高	厂商已发布漏洞修复程序，请及时关注更新：https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=bf9272a92f3df1e4ccfaad434e123222ae5313f7
CNVD-2019-06167	Trend Micro Antivirus for Mac 提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://esupport.trendmicro.com/en-US/home/pages/technical-support/1121296.aspx
CNVD-2019-06187	CA Unified Infrastructure Management 硬编码密码短语漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.ca.com/us/product-content/recommended-reading/security-notices/ca20180829-02--security-notice-for-ca-unified-infrastructure-mgt.html
CNVD-2019-06191	Schneider Electric Modicon M221 密码解码漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.schneider-electric.com/en/product-range-download/62128-logic-controller---modicon-m221#tabs-top
CNVD-2019-06233	Artifex Ghostscript 未初始化内存访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://git.ghostscript.com/?p=ghostpdl.git;a=commit;h=8e9ce5016db968b40e4ec255a3005f2786cce45f
CNVD-2019-06622	ZTE ZXR10 1800-2S ZSRV2 验证绕过漏洞	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=1008723
CNVD-2019-06638	Ansible mysql_user 模块输入验证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/ansible/ansible-modules-core/pull/5388

小结：本周，Cisco 被披露存在多个漏洞，攻击者可利用漏洞攻击者可利用漏洞实施中间人攻击，查看并修改敏感信息，提升权限，执行任意命令，发起拒绝服务攻击等。此外，Linux、IBM、Moxa 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，伪造 URL，实施钓鱼攻击，获取敏感信息，向 Web UI 中注入任意的 JavaScript 代码，发起拒绝服务攻击等另外，Dell EMC RSA Archer 被披露存在信息泄露漏洞。攻击者可利用该漏洞泄露信息。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、FiberHome Fiberhome AN5506-04-F 跨站脚本漏洞

验证描述

FiberHome Fiberhome AN5506-04-F 是一款路由器。

Fiberhome AN5506-04-F RP2669 版本中存在跨站脚本漏洞，该漏洞源于程序未能正确地过滤用户的输入。远程攻击者可利用该漏洞以 Web 应用程权限运行恶意的数据。

验证信息

POC 链接：https://www.exploit-db.com/exploits/46498

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-06340

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. Android TV 曝出 bug 或导致用户私人照片泄露

近日，Twitter 网友 prashanth 爆料称，发现 Android TV 的一个 bug，或导致用户私人照片被泄露。当他连接到一台 Vu Android TV、并选择“切换其他账号”时，竟然能够查看到所有用过这台电视的人的名字和头像。由 prashanth 晒出的视频可知，你还可以通过 Android TV 的幻灯片功能，来查看其他用户的私人照片。

参考链接：https://www.solidot.org/story?sid=59784

2. IBM：访客管理系统存在漏洞，黑客可潜入敏感区域

据媒体报道，IBM 安全研究人员发现，在最流行的 5 大访客管理系统中有 19 个漏洞，黑客可以利用漏洞窃取相关数据，甚至可以潜入办公大楼敏感、禁止区域。IBM 检查了五大流行系统，分别是 Lobby Track Desktop、eVisitorPass（最近将品牌换成了 Threshold Security）、EasyLobby Solo、Passport 和 The Receptionist，它们分别有 7 个、5 个、4 个、2 个和 1 个漏洞。入侵者可以利用漏洞下载访客日志，掌握姓名、驾照、社保数据及手机号等信息；利用有的漏洞甚至可以进入底层操作系统，连线之后就能跳到其它应用和网络。更糟糕的是，入侵者甚至可以获得默认管理证书，完全控制应用，比如编辑访客数据库。

参考链接：https://www.bianews.com/news/flash?id=32315

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