国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 11 月 04 日-2019 年 11 月 10 日 **2019 年第 45 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 425 个，其中高危漏洞 105 个、中危漏洞 259 个、低危漏洞 61 个。漏洞平均分值为 5.60。本周收录的漏洞中，涉及 0day 漏洞 80 个（占 19%），其中互联网上出现“D-Link DIR-859 和 DIR-850L 命令注入漏洞、ClonOS WEB control panel 跨站脚本漏洞”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 7452 个，与上周（8002 个）环比减少 7%。

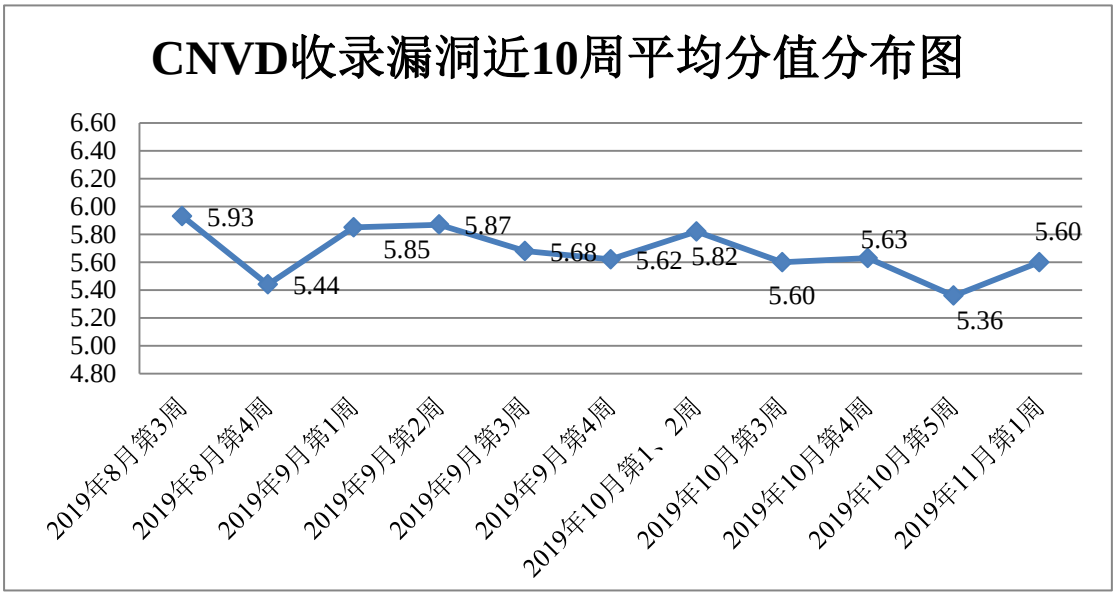


图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 3 起，向基础电信企业通报漏洞事件 0 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 635 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 125 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 21 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：

龙采科技（山西）有限公司、青岛易软天创网络科技有限公司、济南点创网络科技有限公司、广州合优网络科技有限公司、洛阳万谦网络科技有限公司、上海秀视智能科技有限公司、成都思乐科技有限公司、深圳迪元素科技有限公司、深圳搜豹网络有限公司、淄博闪灵网络科技有限公司、重庆楚捷科技有限公司、成都乘龙文化传媒有限公司、西安佰联网络技术有限公司、施耐德电气(中国)有限公司、十堰八五科技有限公司、长春凌展软件有限责任公司、中国国旅股份有限公司、北京新诚软科技有限公司、上海开杰信息技术有限公司、中铁八局集团有限公司、中铁五局集团置业有限公司、南京国格信息科技有限公司、成都依能科技股份有限公司、中国电器科学研究院股份有限公司、深圳市蓝色航线科技有限公司、北京库巴扎信息科技有限公司、沈阳盘古网络技术有限公司、帆软软件有限公司、青岛易软天创网络科技有限公司、深圳市锟铻科技有限公司、北京网御星云信息技术有限公司、武汉百捷集团信息科技股份有限公司、兴证国际金融集团有限公司、上海企炬广告传媒有限公司、昆明云涛科技有限公司、灵吉网络科技有限公司、中国水利电力质量管理协会、北京审信核信企业信用评估中心、辽宁省银行协会、MyfCMS-闵益飞内容管理系统、国家人类遗传资源中心、HadSky、一站科技、XnSoft、苹果 CMS、ShopXO、Zzzcms、Kitecms、PHPEMS、Gxlcms、ZZCMS、Xnview、Phpmywind、Cleanersoft、信呼、Pluck CMS、Sonatype、乐尚商城开源系统、Waychar、熊海 CMS、JeePlus 和海洋 CMS。

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、哈尔滨安天科技集团股份有限公司、深信服科技股份有限公司、华为技术有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、北京华云安信息技术有限公司、山东云天安全技术有限公司、山东新潮信息技术有限公司、杭州海康威视数字技术股份有限公司、广州蕴辰网络科技有限公司、新疆海狼科技有限公司、北京君信安科技有限公司、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、腾讯安全云鼎实验室、内蒙古奥创科技有限公司、北京智游网安科技有限公司、江苏安又恒信息科技有限公司、雷石安全实验室、山东云天安全大数据技术有限公司及其他个人白帽子向 CNVD 提交了 7452 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 6645 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
奇安信网神（补天平台）	4664	4664
斗象科技（漏洞盒子）	1520	1520
上海交大	461	461
北京天融信网络安全技术有限公司	253	1
哈尔滨安天科技集团股份有限公司	207	0
深信服科技股份有限公司	110	3
华为技术有限公司	105	0
新华三技术有限公司	58	0
恒安嘉新(北京)科技股份公司	49	49
北京启明星辰信息安全技术有限公司	47	0
北京神州绿盟科技有限公司	34	1
四川无声信息技术有限公司	28	28
中国电信集团系统集成有限责任公司	21	21
北京数字观星科技有限公司	20	0
厦门服云信息科技有限公司	19	1
北京知道创宇信息技术股份有限公司	4	4
远江盛邦（北京）网络安全科技股份有限公司	126	126
国瑞数码零点实验室	109	109
北京华云安信息技术有限公司	48	48
山东云天安全技术有限公司	27	27
山东新潮信息技术有限公司	22	22

杭州海康威视数字技术股份有限公司	10	10
广州蕴辰网络科技有限公司	9	9
新疆海狼科技有限公司	9	9
北京君信安科技有限公司	6	6
河南信安世纪科技有限公司	4	4
山东华鲁科技发展股份有限公司	3	3
腾讯安全云鼎实验室	3	3
内蒙古奥创科技有限公司	1	1
北京智游网安科技有限公司	1	1
江苏安又恒信息科技有限公司	1	1
雷石安全实验室	1	1
山东云天安全大数据技术有限公司	1	1
CNCERT 西藏分中心	7	7
CNCERT 四川分中心	5	5
CNCERT 浙江分中心	3	3
个人	303	303
报送总计	8299	7452

本周漏洞按类型和厂商统计

本周，CNVD 收录了 425 个漏洞。应用程序 295 个，网络设备（交换机、路由器等网络端设备）48 个，操作系统 41 个，WEB 应用 15 个，安全产品 12 个，数据库 8 个，智能设备（物联网终端设备）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	295
网络设备（交换机、路由器等网络端设备）	48

操作系统	41
WEB 应用	15
安全产品	12
数据库	8
智能设备（物联网终端设备）	6

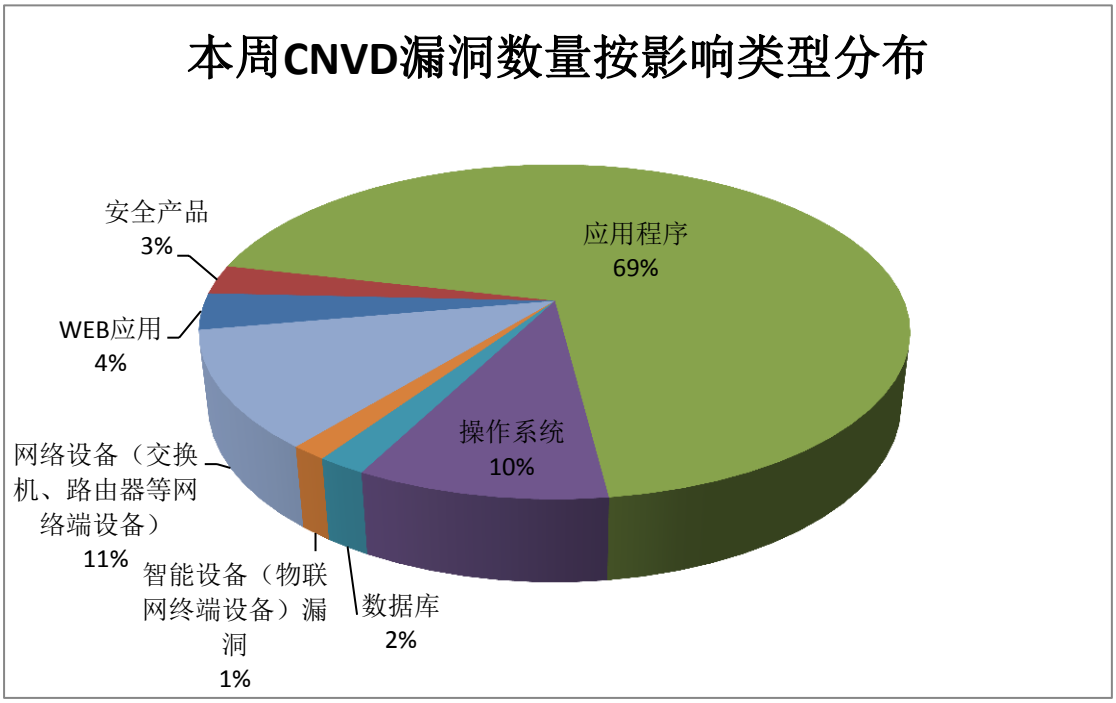


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Cisco、Google 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	Oracle	80	19%
2	Cisco	45	11%
3	Google	37	9%
4	D-Link	25	6%
5	Microsoft	25	6%
6	IBM	19	4%
7	Magento	15	4%
8	Adobe	12	3%
9	Eclipse	10	2%
10	其他	157	36%

本周行业漏洞收录情况

本周，CNVD 收录了 28 个电信行业漏洞，41 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Schneider Electric Modicon M580 拒绝服务漏洞、多款 D-Link 产品命令注入漏洞、Google Android System 权限提升漏洞（CNVD-2019-39720）、Cisco Aironet Access PPTP 拒绝服务漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，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/

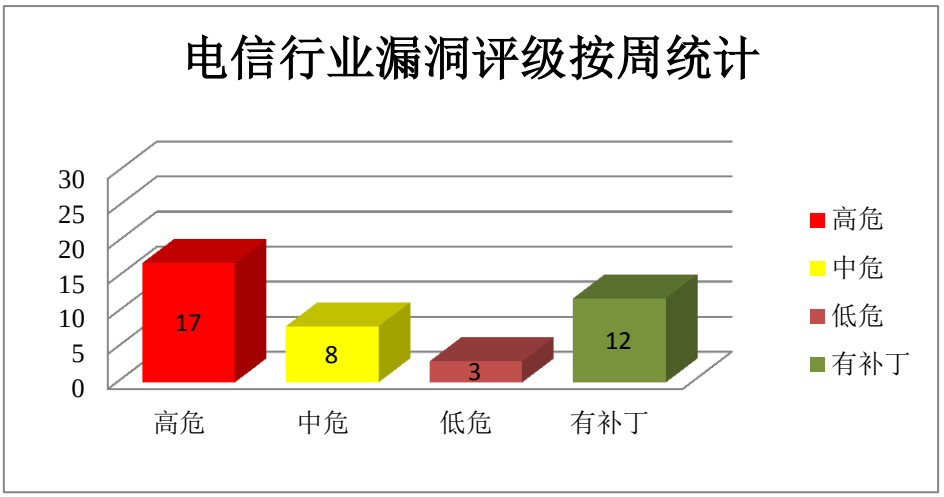


图 3 电信行业漏洞统计

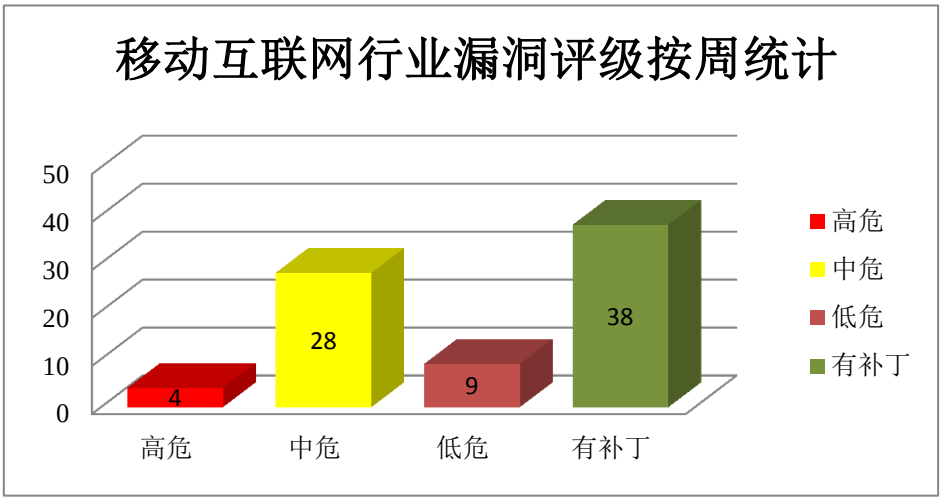
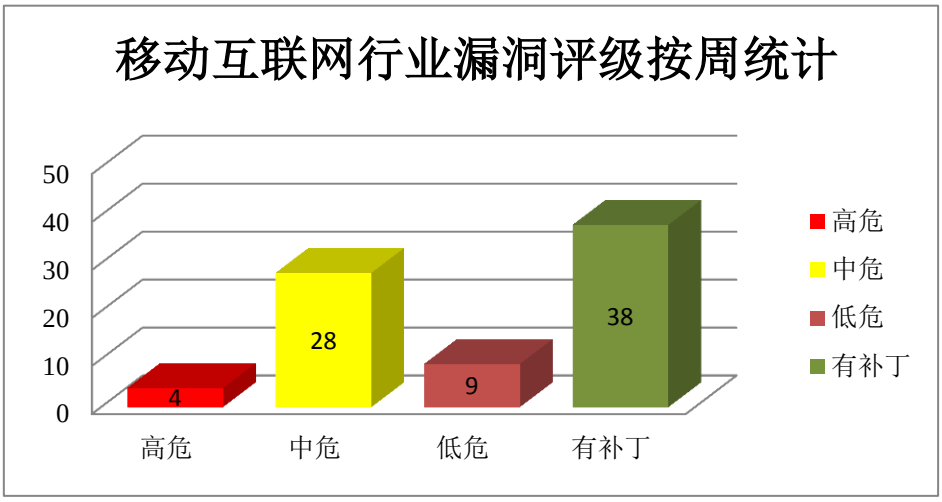


图 4 移动互联网行业漏洞统计



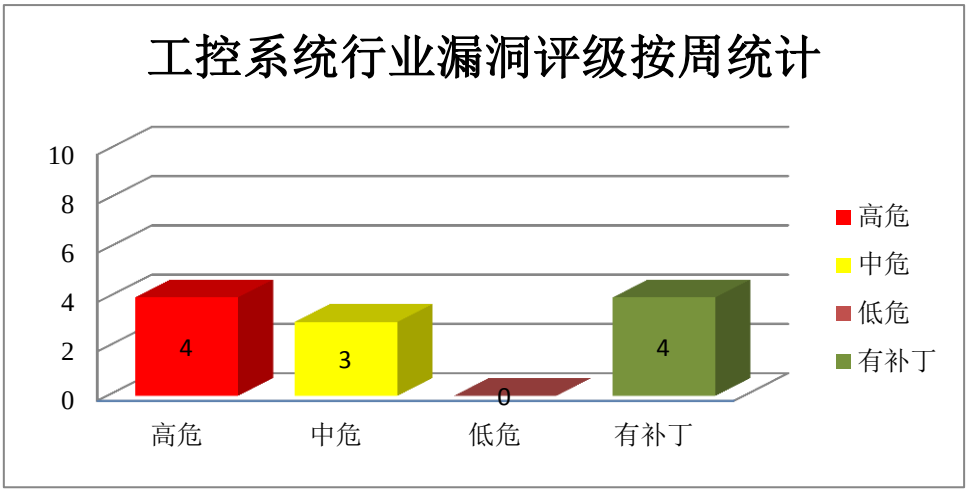


图 5 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco Enterprise NFV Infrastructure Software 是一款轻量级虚拟化平台，将完整的 VM 生命周期管理、监控、设备可编程性及服务链集成在了一个可安装的软件包中。Cisco Aironet AP 是一系列访问接入点产品。Cisco Video Communications Server（VCS）是一款用于视频会议解决方案的视频通信服务器。Cisco Enterprise Chat and Email（CEC）是一套企业聊天和电子邮件解决方案。Cisco Wireless LAN Controller（WLC）Software 是一套用于配置和管理 WLC（无线局域网控制器）的软件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞执行任意命令，造成拒绝服务。

CNVD 收录的相关漏洞包括：Cisco Enterprise NFV Infrastructure Software 命令注入漏洞（CNVD-2019-38848、CNVD-2019-38855）、Cisco Enterprise NFV Infrastructure Software 任意文件读写漏洞、Cisco Enterprise NFV Infrastructure Software VNC 认证

绕过漏洞、Cisco Aironet Access PPTP 拒绝服务漏洞、Cisco Video Communications Server 命令注入漏洞、Cisco Enterprise Chat and Email 跨站脚本漏洞（CNVD-2019-39701）、Cisco Wireless LAN Controller Software 输入验证错误漏洞（CNVD-2019-39768）。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-2019-38848
http://www.cnvd.org.cn/flaw/show/CNVD-2019-38854
http://www.cnvd.org.cn/flaw/show/CNVD-2019-38855
http://www.cnvd.org.cn/flaw/show/CNVD-2019-38858
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39607
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39608
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39701
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39768

2、Microsoft 产品安全漏洞

Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以当前用户的权限运行任意代码。。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 脚本引擎内存破坏漏洞（CNVD-2019-39009、CNVD-2019-39013、CNVD-2019-39011、CNVD-2019-39012、CNVD-2019-39014、CNVD-2019-39015）、Microsoft Internet Explorer VBScript 引擎缓冲区溢出漏洞（CNVD-2019-39010）、Microsoft Internet Explorer VBScript 引擎远程内存破坏漏洞（CNVD-2019-39018）。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-2019-39009
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39010
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39013
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39011
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39012
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39014
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39015
http://www.cnvd.org.cn/flaw/show/CNVD-2019-39018

3、Google 产品安全漏洞

Chrome OS 是美国谷歌（Google）的一套基于 Web 的轻量型开源操作系统。Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）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，攻击者可利用漏洞提升权限，造成拒

绝服务。

CNVD 收录的相关漏洞包括：Google Android Framework 拒绝服务漏洞（CNVD-2019-38873）、Google Android Framework 权限提升漏洞（CNVD-2019-38878、CNVD-2019-38881、CNVD-2019-38882、CNVD-2019-38883、CNVD-2019-39720）、Google Chrome OS Imagination Technologies driver 输入验证错误漏洞、Google Android System 缓冲区溢出漏洞（CNVD-2019-39716）。其中，除“Google Android Framework 权限提升漏洞（CNVD-2019-38878、CNVD-2019-38881、CNVD-2019-38882）”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-2019-38873

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38878

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38881

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38882

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38883

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39672

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39716

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39720

4、IBM 产品安全漏洞

IBM Cloud Orchestrator 是一套为云管理解决方案。IBM API Connect（APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM OpenPages GRC Platform 是一套用于管理企业风险和合规性的平台。IBM InfoSphere Information Server 是美一套数据整合平台。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，向 Web UI 中注入任意的 JavaScript 代码。

CNVD 收录的相关漏洞包括：IBM Cloud Orchestrator 跨站脚本漏洞、IBM Cloud Orchestrator 信息泄露漏洞（CNVD-2019-39203、CNVD-2019-39207）、IBM Cloud Orchestrator 路径遍历漏洞、IBM API Connect 信息泄露漏洞（CNVD-2019-39355）、IBM OpenPages GRC Platform 跨站脚本漏洞（CNVD-2019-39353）、IBM OpenPages GRC Platform 信息泄露漏洞（CNVD-2019-39354）、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-2019-39757）。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-2019-39204

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39203

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39206

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39207

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39355

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39353

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39354

http://www.cnvd.org.cn/flaw/show/CNVD-2019-39757

5、Philips IntelliSpace Perinatal 未授权访问漏洞

Philips IntelliSpace Perinatal 是一套用于医疗行业的产科护理信息管理解决方案。本周，Philips IntelliSpace Perinatal 被披露存在未授权访问漏洞。攻击者可利用该漏洞绕过应用程序的限制，访问 Windows 操作系统中未授权的信息。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-2019-39582

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-2019-38863	Intel Unite Client 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://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00245.html
CNVD-2019-38871	Schneider Electric Modicon M580 拒绝服务漏洞	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.schneider-electric.com/en/download/document/SEVD-2019-134-11
CNVD-2019-39165	SUSE Supportutils 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.suse.com/support/update/announcement/2019/suse-su-20190480-1
CNVD-2019-39174	JetBrains TeamCity Java 反序列化漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://blog.jetbrains.com/blog/2019/10/29/jetbrains-security-bulletin-q3-2019/
CNVD-2019-39393	Magento 代码执行漏洞（CNVD-2019-39393）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://magento.com/security/patches/magento-2.3.2-2.2.9-and-2.1.18-security-update-13
CNVD-2019-39592	Adobe Download Manager 不安全文件权限漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/adm/apsb19-51.html
CNVD-201	LibreOffice 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏

9-39680			洞，补丁获取链接：https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9850
CNVD-2019-39690	Linux kernel 内存泄漏漏洞（CNVD-2019-39690）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.mail-archive.com/linux-kernel@vger.kernel.org/msg1935698.html
CNVD-2019-39761	ZTE 9000E 权限许可和访问控制问题漏洞	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=1011682
CNVD-2019-39874	TightVNC 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.tightvnc.com

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意命令，造成拒绝服务。此外，Microsoft、Google、IBM 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，造成拒绝服务等。另外，Philips IntelliSpace Perinatal 被披露存在未授权访问漏洞。攻击者可利用该漏洞绕过应用程序的限制，访问 Windows 操作系统中未授权的信息。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、D-Link DIR-859 和 DIR-850L 命令注入漏洞

验证描述

D-Link DIR-859 是一款无线 AC1750 大功率 Wi-Fi 千兆路由器。D-Link DIR-850L 是一款无线 AC1200 双频千兆云路由器。

D-Link DIR-859 A3-1.06 和 DIR-850L A1.13 中的/etc/services/DEVICE.TIME.php 存在命令注入漏洞。攻击者可通过$SERVER 变量利用该漏洞实现远程代码执行。

验证信息

POC 链接：https://github.com/dahua966/Routers-vuls/tree/master/DIR-859

参考链接： https://www.cnvd.org.cn/flaw/show/CNVD-2019-39550

信息提供者

华为技术有限公司

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. Libarchive 库中的一个漏洞影响了主要 Linux 发行版

Google 专家在压缩库 libarchive 中发现了一个漏洞，为 CVE-2019-18408，可能导致任意代码执行。libarchive 库是一种多格式的存档和压缩库，它实现用于读取/写入各种压缩格式的单个接口。该漏洞影响主要的 Linux 发行版，包括 Debian，Ubuntu，Arch Linux，FreeBSD 和 NetBSD。

参考链接：https://securityaffairs.co/wordpress/93507/hacking/libarchive-library-flaw.html

2. Epic 商城再次曝出 DRM 漏洞

最近 CCN 的安全研究员曝光了 Epic 商城的又一个安全漏洞：玩家即使没购买过游戏，也可以无障碍游玩。研究员在多台设备上测试了这个漏洞，只要持有游戏的账号登陆了这台设备并安装了游戏，那么这台设备上所有用户都能运行游戏。Epic 商城依靠低分成和巨额独占费，获得了不少游戏大作的先发权，比如《天外世界》《无主之地 3》《荒野大镖客 2》等等。

参考链接：https://www.dbsec.cn/blog/article/5360.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