国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 12 月 02 日-2019 年 12 月 08 日 **2019 年第 49 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 481 个，其中高危漏洞 220 个、中危漏洞 238 个、低危漏洞 23 个。漏洞平均分值为 6.34。本周收录的漏洞中，涉及 0day 漏洞 309 个（占 64%），其中互联网上出现“WordPress Plainview Activity Monitor 远程命令执行漏洞、pfSense 跨站请求伪造漏洞（CNVD-2019-43356）”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 2338 个，与上周（1893 个）环比增长 24%。

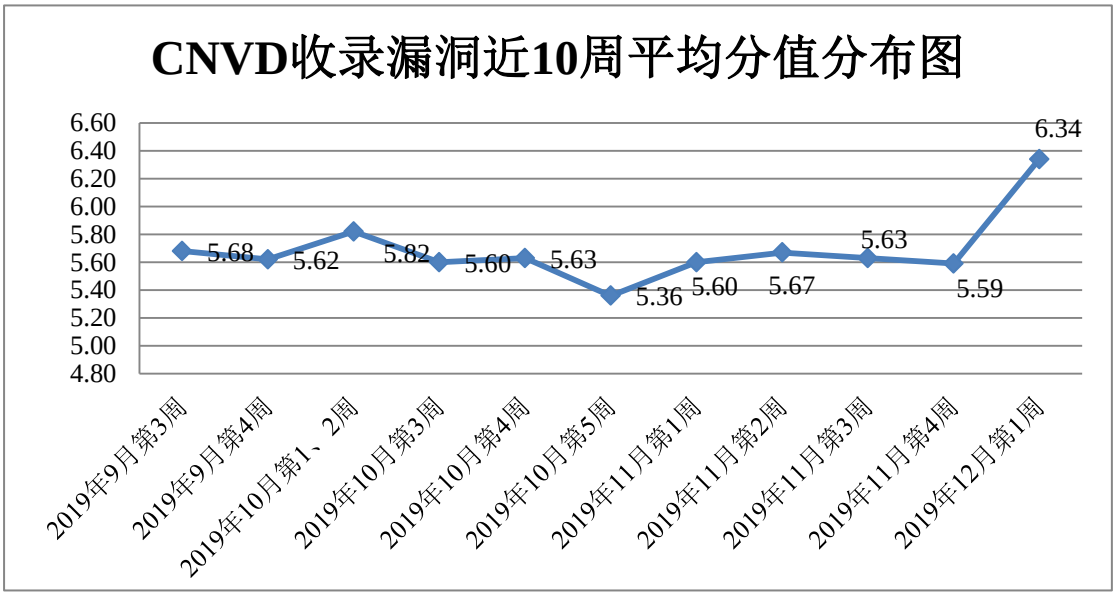

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 起，向基础电信企业通报漏洞事件 9 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 224 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 52 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 17 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：

河北鑫考教育科技股份有限公司、洪湖尔创网联信息技术有限公司、东莞市宇腾信息科技有限公司、上海企炬广告传媒有限公司、河北品科信息科技有限公司、武汉海昌信息技术有限公司、微软(中国)有限公司、黑龙江资海科技集团股份有限公司、广州红帆科技有限公司、成都康菲顿特网络科技有限公司、福建福昕软件开发股份有限公司、北京京东世纪贸易有限公司、深圳乐播科技有限公司、北京小米科技有限责任公司、浙江翼信科技有限公司、北京致远互联软件股份有限公司、湖南潭州教育网络科技有限公司、北京车之家信息技术有限公司、衡水金航计算机科技有限公司、沧州市凡诺广告传媒有限公司、山西先启科技有限公司、广联达科技股份有限公司、洛阳云业信息科技有限公司、深圳迪元素科技有限公司、长沙米拓信息技术有限公司、深圳市锟铻科技有限公司、北京良精志诚科技有限责任公司、上海泛微网络科技股份有限公司、明博教育科技股份有限公司、西安博信信息科技有限公司、镇江市云优网络科技有限公司、北京网易有道计算机系统有限公司京五八信息技术有限公司、京优贝在线网络科技有限公司、广州华多网络科技有限公司、上海勤和互联网技术软件开发有限公司、广州网易计算机系统有限公司、北京二六三企业通信有限公司、浙江齐聚科技有限公司、深圳市迪元素科技有限公司、上海互盾信息科技有限公司、山西牛酷信息科技有限公司、山西企凝信息科技有限公司、邢台腾和网络科技有限公司、南充市老虎云网络技术有限公司、上海发那科机器人有限公司、名炬企业管理（上海）有限公司、北京奥泰瑞格科技有限公司、哈尔滨伟成科技有限公司、海南易而优科技有限公司、北京东土科技股份有限公司、中国管理科学研究院企业管理创新研究所、中国管理科学研究院、海尔集团、乘风原创程序、金融说直播云平台、天人系列管理系统、超级 CMS、梦想 CMS、易贝 CMS、zzzcms、X5music、Oracle、iPubsoft Studio、zzcms、Popojicms、ZhiCms、Jobberbase、SchoolCMS、WellCMS、The Apache Software Foundation、KiteCMS、Digi International Inc 和 KUKA。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京知道创宇信息技术股份有限公司、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、深信服科技股份有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。北京铭图天成信息技术有限公司、内蒙古洞明科技有限公司、南京众智维信息科技有限公司、山东新潮信息技术有限公司、山东云天安全技术有限公司、河南灵创电子科技有限公司、内蒙古奥创科技

有限公司、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、新疆海狼科技有限公司、广州蕴辰网络科技有限公司、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、北京圣博润高新技术股份有限公司、上海端御信息科技有限公司、杭州海康威视数字技术股份有限公司、内蒙古迅如信息安全科技有限公司、腾讯安全科恩实验室及其他个人白帽子向 CNVD 提交了 2338 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 1490 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）	744	744
奇安信网神（补天平台）	413	413
上海交大	333	333
北京知道创宇信息技术股份有限公司	225	225
哈尔滨安天科技集团股份有限公司	216	0
北京天融信网络安全技术有限公司	108	10
深信服科技股份有限公司	101	0
华为技术有限公司	99	0
北京神州绿盟科技有限公司	84	0
北京启明星辰信息安全技术有限公司	53	5
恒安嘉新(北京)科技股份公司	52	0
新华三技术有限公司	49	0
四川无声信息技术有限公司	25	25
北京数字观星科技有限公司	17	0
西安四叶草信息技术有限公司	11	11
沈阳东软系统集成工程有限公司	2	2

国家互联网应急中心	2	2
北京铭图天成信息技术有限公司	55	55
内蒙古洞明科技有限公司	45	45
南京众智维信息科技有限公司	39	39
山东新潮信息技术有限公司	33	33
山东云天安全技术有限公司	26	26
河南灵创电子科技有限公司	22	22
内蒙古奥创科技有限公司	20	20
远江盛邦（北京）网络安全科技股份有限公司	19	19
国瑞数码零点实验室	14	14
杭州迪普科技股份有限公司	14	0
新疆海狼科技有限公司	8	8
广州蕴辰网络科技有限公司	6	6
河南信安世纪科技有限公司	5	5
山石网科通信技术股份有限公司	5	5
北京圣博润高新技术股份有限公司	2	2
上海端御信息科技有限公司	2	2
杭州海康威视数字技术股份有限公司	1	1
内蒙古迅如信息安全科技有限公司	1	1
腾讯安全科恩实验室	1	1
CNCERT 四川分中心	5	5
CNCERT 西藏分中心	3	3

CNCERT 吉林分中心	2	2
个人	254	254
报送总计	3116	2338

本周漏洞按类型和厂商统计

本周，CNVD 收录了 481 个漏洞。WEB 应用 243 个，应用程序 170 个，操作系统 29 个，网络设备（交换机、路由器等网络端设备）17 个，安全产品 11 个，智能设备（物联网终端设备）10 个和数据库 1 个个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
WEB 应用	243
应用程序	170
操作系统	29
网络设备（交换机、路由器等网络端设备）	17
安全产品	11
智能设备（物联网终端设备）	10
数据库	1

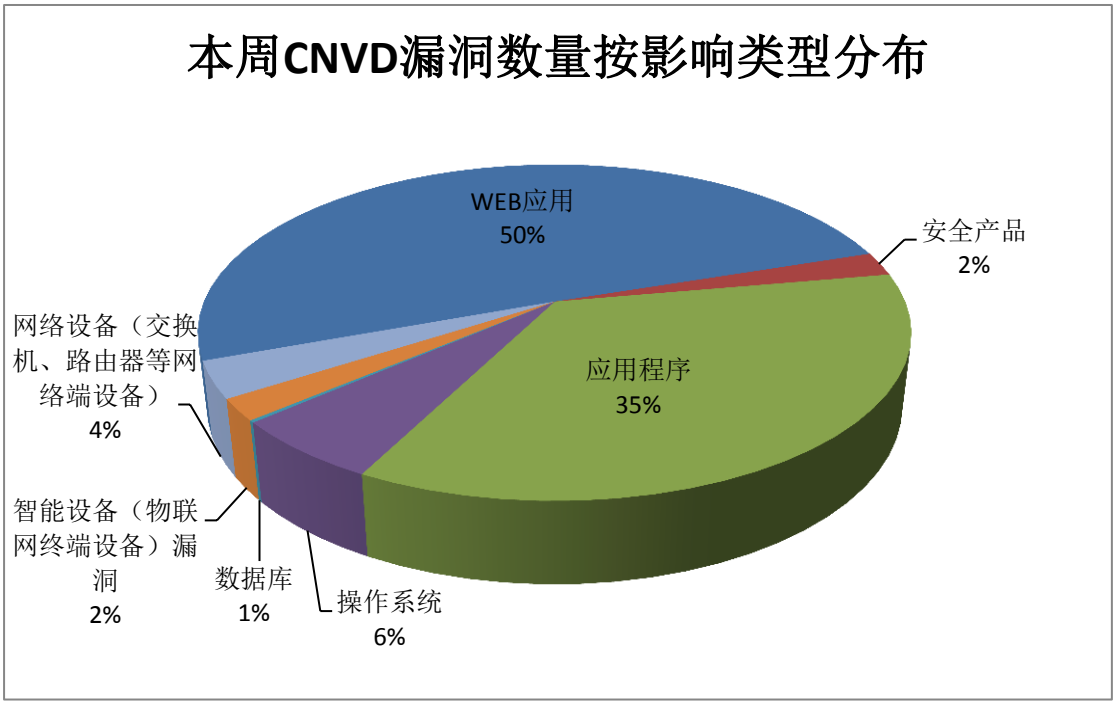

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及海洋 CMS、Google、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	海洋 CMS	37	8%
2	Google	21	5%
3	IBM	19	4%
4	Cisco	11	2%
5	HP	11	2%
6	Cloud Foundry	10	2%
7	MyuCMS 社区	7	1%
8	FusionPBX	6	1%
9	Moodle	6	1%
10	其他	353	74%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，51 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，“Google Android Media Framework 远程代码执行漏洞（CNVD-2019-44275）、AVEVA Group plc InduSoft Web Studio 和 InTouch Edge HMI 存在未明漏洞、phpipam SQL 注入漏洞（CNVD-2019-43861）、Google Android Framework 权限提升漏洞（CNVD-2019-44279）”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/

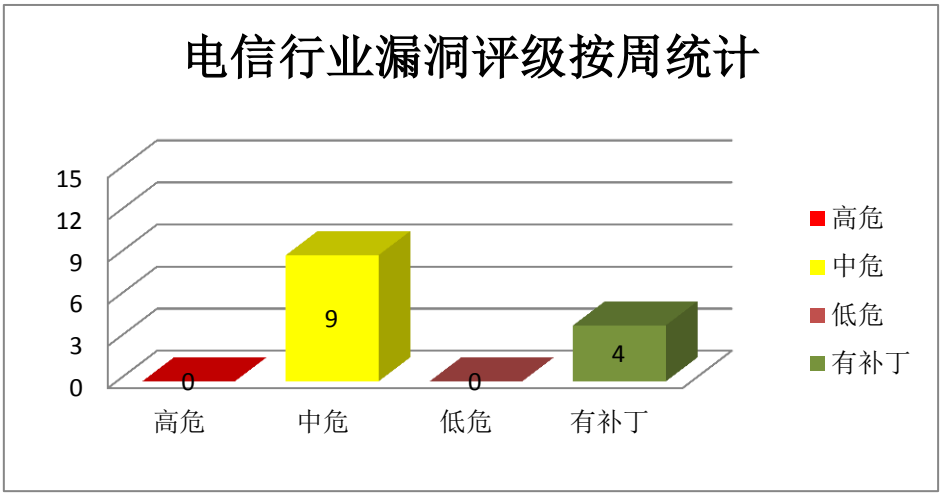

图 3 电信行业漏洞统计

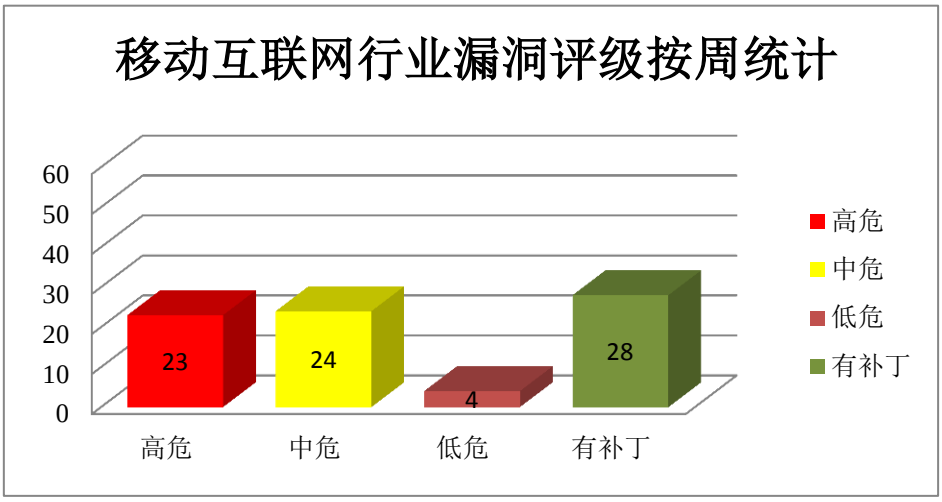

图 4 移动互联网行业漏洞统计

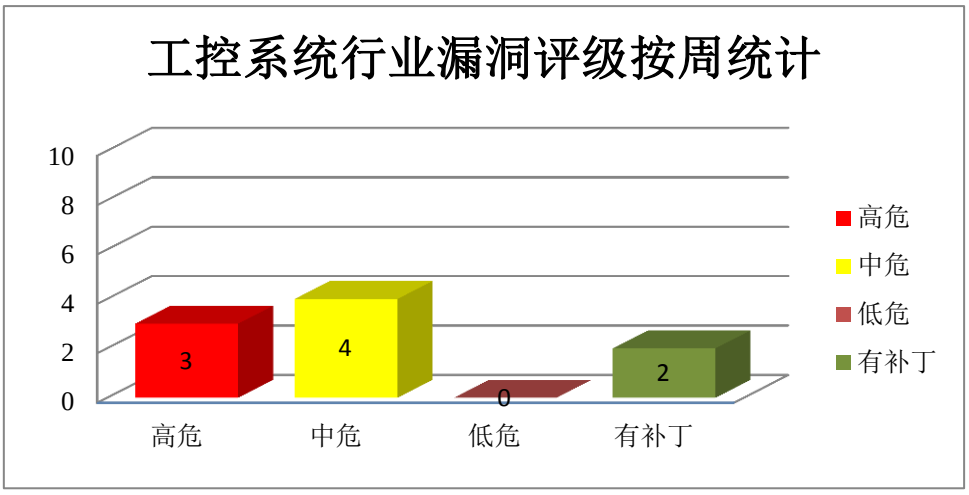

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

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权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限，执行代码。

CNVD 收录的相关漏洞包括：Google Android Framework 权限提升漏洞（CNVD-2019-44265、CNVD-2019-44277、CNVD-2019-44278、CNVD-2019-44279）、Google Android Media Framework 远程代码执行漏洞（CNVD-2019-44273、CNVD-2019-44275）、Google Android System 权限提升漏洞（CNVD-2019-44274）、Google Android System 远程代码执行漏洞（CNVD-2019-44276）。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-2019-44265

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44277

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44278

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44279

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44273

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44275

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44274

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44276

2、IBM 产品安全漏洞

IBM Security Identity Manager（ISIM）是一套身份管理和治理解决方案。IBM Spectrum Protect Backup-Archive Client 是一套用于 IBM Spectrum Protect 文件备份、归档的客户端程序。IBM Cloud Pak System 是一套具有可配置、预集成软件的全栈、融合基础架构。IBM Streams 是一套实时数据分析解决方案。IBM Content Navigator 是一款 Web 客户机。IBM Tivoli Netcool Impact 是一套网络管理软件。IBM Operations Analytics-Log Analysis 是一套半结构化数据分析解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过客户端验证，获取敏感信息，执行任意代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：IBM Security Identity Manager 任意代码执行漏洞、IBM Spectrum Protect Backup-Archive Client 拒绝服务漏洞、IBM Cloud Pak System 客户端验证漏洞、IBM InfoSphere Streams 信息泄露漏洞、IBM Content Navigator 信息泄露漏洞、IBM Tivoli Netcool Impact 信息泄露漏洞、IBM Operations Analytics-Log Analysis 信息泄露漏洞、IBM Cloud Pak System 任意文件上传漏洞。其中，“IBM Security Identity Manager 任意代码执行漏洞、IBM Cloud Pak System 任意文件上传漏洞”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-2019-43051

http://www.cnvd.org.cn/flaw/show/CNVD-2019-43052

http://www.cnvd.org.cn/flaw/show/CNVD-2019-43055

http://www.cnvd.org.cn/flaw/show/CNVD-2019-43892

http://www.cnvd.org.cn/flaw/show/CNVD-2019-43894

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44127

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44134

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44251

3、Cisco 产品安全漏洞

Cisco Email Security Appliance（ESA）是一个电子邮件安全设备。AsyncOS Software 是运行在其中的一套操作系统。Cisco IOS XR 是一套为其网络设备开发的操作系统。Cisco Webex Meeting Center 是一套在线协作视频会议解决方案。Cisco Webex Event Center 是一套网络研讨和在线活动管理平台。Cisco Webex Support Center 是一套针对服务支持团队的视频会议解决方案。Cisco Small Business RV Series Routers 是一款 RV 系列路由器。Cisco DNA Spaces 是一套室内定位服务平台。Cisco DNA Spaces:Connector 是其中的一个用于支持 Cisco 无线控制器通信的连接器。Cisco Stealthwatch Enterprise 是一套企业网络安全防护解决方案。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，提升权限等。

CNVD 收录的相关漏洞包括：Cisco Email Security Appliance AsyncOS Software 输入验证错误漏洞、Cisco IOS XR 访问控制错误漏洞、多款 Cisco 产品信息泄露漏洞（CNVD-2019-44128）、Cisco Small Business RV Series Routers 信息泄露漏洞、Cisco DNA Spaces:Connector 权限许可和访问控制问题漏洞、Cisco DNA Spaces:Connector 输入验证错误漏洞、Cisco DNA Spaces:Connector SQL 注入漏洞、Cisco Stealthwatch Enterprise 跨站脚本漏洞。其中，“Cisco DNA Spaces:Connector 权限许可和访问控制问题漏洞、Cisco DNA Spaces:Connector 输入验证错误漏洞、Cisco DNA Spaces:Connector SQL 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-2019-43819
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43820
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44128
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44135
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44283
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44284
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44285
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44286

4、HP 产品安全漏洞

HP ThinPro Linux 是一套用于 HP 瘦客户机的操作系统。HP Workstation 是一款高性能台式电脑。BIOS 是其中的一个基本输入输出系统。HP Service Pack for ProLiant 是一个全面的系统软件和固件更新解决方案。HP Support Assistant 是一套为 PC 和打印机提供支持等功能的解决方案。HP Remote Graphics Software 是一款远程桌面图形软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过某些安全限制并获得数据的未授权访问权限，篡改运行时 BIOS 代码，执行任意代码等。

CNVD 收录的相关漏洞包括：HP ThinPro Linux 权限提升漏洞、HP ThinPro Linux 任意代码执行漏洞（CNVD-2019-43732、CNVD-2019-43734、CNVD-2019-43735）、H

P Workstation BIOS 安全特征问题漏洞、HP Service Pack for ProLiant 本地未授权访问漏洞、HP Support Assistant 授权问题漏洞、HP Remote Graphics Software 信任管理问题漏洞。其中，“HP ThinPro Linux 权限提升漏洞、HP ThinPro Linux 任意代码执行漏洞（CNVD-2019-43734、CNVD-2019-43735）、HP Workstation BIOS 安全特征问题漏洞”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-2019-43731
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43732
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43734
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43735
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43896
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43897
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43899
http://www.cnvd.org.cn/flaw/show/CNVD-2019-43900

5、Red Hat FreeIPA 访问控制绕过漏洞

Red Hat FreeIPA 是美国红帽（Red Hat）公司的一套集成的安全信息管理解决方案。本周，Red Hat FreeIPA 被披露存在访问控制绕过漏洞。攻击者可利用该漏洞绕过访问限制。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-2019-43670

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-2019-43359	Netskope Client 命令注入漏洞	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.netskope.com
CNVD-2019-43385	Advantech WISE-PaaS/RMM 未授权访问漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.advantech.com
CNVD-2019-43399	Eclipse Vert.xXML 外部实体注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bugs.eclipse.org/bugs/show_bug.cgi?id=539568
CNVD-2019-43836	Ignite Realtime Openfire 服务器端请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/igniterealtime/Openfire/pull/1497
CNVD-201	Cloud Foundry UAA SCIM 权	高	厂商已发布了漏洞修复程序，请及时

9-43844	限提升漏洞		关注更新：https://www.cloudfoundry.org/blog/cve-2019-11278/
CNVD-2019-43848	NetApp ONTAP Select Deploy 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.netapp.com/advisory/ntap-20191121-0001/
CNVD-2019-43858	Aruba ClearPass Policy Manager 命令执行漏洞	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.arubanetworks.com/assets/alert/ARUBA-PSA-2018-007.txt
CNVD-2019-44138	Cloud Foundry Routing输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.cloudfoundry.org/blog/cve-2019-11289
CNVD-2019-44226	Ubiquiti Networks UniFi Video Controller 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ui.com
CNVD-2019-44258	Crestron Electronics DMC-STRO 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.crestron.com

小结：本周，Google 产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限，执行代码。此外，IBM、Cisco、HP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过客户端验证，获取敏感信息，提升权限，执行任意代码，造成拒绝服务。另外，Red Hat FreeIPA 被披露存在访问控制绕过漏洞。攻击者可利用该漏洞绕过访问限制。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、WordPress Plainview Activity Monitor 远程命令执行漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。Plainview Activity Monitor 是使用在其中的一个网站用户活动监控插件。

WordPress Plainview Activity Monitor 存在远程命令执行漏洞。攻击者可利用该漏洞在底层系统上远程执行命令。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2019110179

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2019-44249

信息提供者

深信服科技股份有限公司

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. Strandhogg 漏洞：Android 系统上的维京海盗

StrandHogg 是一个存在于 Android 多任务系统中的应用漏洞。该漏洞利用则是基于一个名为“taskAffinity”的 Android 控件设置，允许包括恶意应用在内的任意程序，随意采用多任务处理系统中的任何身份。从零日核实的情况来看，StrandHogg 漏洞确实存在于 Android 的多任务系统中，一旦已安装恶意程序利用，就能让恶意程序顺利伪装合法应用，获得更高的权限，窃取信息或进行任意恶意操作。

参考链接：https://www.freebuf.com/news/221933.html

2. GoAhead Web 服务器中的严重漏洞可能影响多数的物联网设备

网络安全研究人员发现了 GoAhead Web 服务器软件中两个新漏洞的详细信息，Go Ahead Web 服务器软件是一个广泛嵌入在数亿个与互联网连接的智能设备中的微型应用程序。其中一个漏洞（CVE-2019-5096）是关键代码执行漏洞，攻击者可以利用此漏洞在易受攻击的设备上执行恶意代码并控制它们。

参考链接：https://thehackernews.com/2019/12/goahead-web-server-hacking.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