国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 10 月 28 日-2019 年 11 月 03 日 **2019 年第 44 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 478 个，其中高危漏洞 92 个、中危漏洞 339 个、低危漏洞 47 个。漏洞平均分值为 5.36。本周收录的漏洞中，涉及 0day 漏洞 101 个（占 21%），其中互联网上出现“Apache Solr 基于 Velocity 模板远程命令执行漏洞、ACTi ACM-5611 Camera 远程命令执行漏洞”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 8002 个，与上周（9602 个）环比减少 17%。

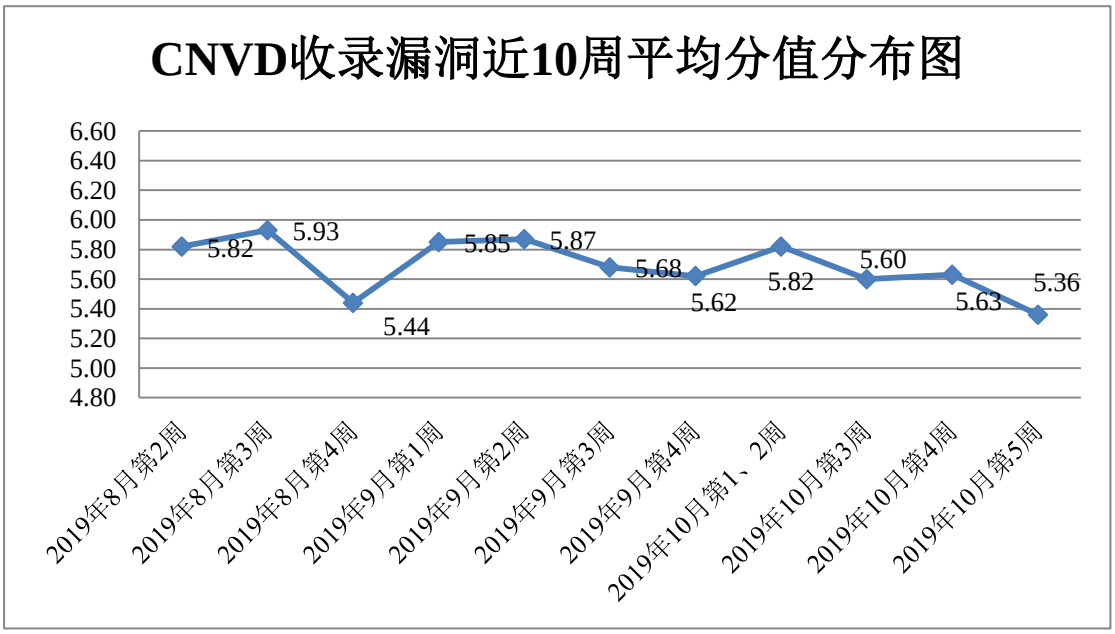

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 23 起，向基础电信企业通报漏洞事件 3 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 578 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 62 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 22 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：

保定市互动企业营销策划有限公司、贵州霹雳云信息科技有限公司、厦门易商网络科技有限公司、合肥司瓦图网络科技有限责任公司、国药集团国瑞药业有限公司、淮南市银泰软件科技有限公司、淄博闪灵网络科技有限公司、青岛易软天创网络科技有限公司、中大英才（北京）网络教育科技有限公司、大连华天软件有限公司、国药集团山西有限公司、帝兴软件开发有限公司、用友网络科技股份有限公司、湖北国昇科技有限公司、北京正量网科技有限公司、深圳市蓝色航线科技有限公司、中国科学院沈阳科学仪器股份有限公司、苏州烟火网络科技有限公司、山西牛酷信息科技有限公司、嘉兴想天信息科技有限公司、北方华锦化学工业集团有限公司、深圳搜豹网络有限公司、廊坊市极致网络科技有限公司、成都今网科技有限公司、中铁二十局集团房地产开发有限公司、徐州梦创信息科技有限公司、上海丹帆网络科技有限公司、上海七慧网络科技有限公司、伟创互联网络技术开发团队、北京佰信安科技有限公司、青岛商至信网络科技有限公司、上海卓卓网络科技有限公司、北京米尔伟业科技有限公司、曲靖市品智科技有限公司、深圳市亚网科技有限公司、淄博汇通电子科技有限公司、北京安天网络安全技术有限公司、施耐德电气(中国)有限公司、惠州市众兴互联科技有限公司、兴证国际金融集团有限公司、北京创联教育投资有限公司、宜兴易发网络服务有限公司、海南赞赞网络科技有限公司、国药控股湖北有限公司、北京亚控科技发展有限公司、中铁置业集团有限公司、无锡时光网络科技有限公司、中国供销集团有限公司、中粮（成都）粮油工业有限公司、百易网络、帝国软件、中国中医科学院中医药科技合作中心、中国社区卫生协会、企业第一网、中国文化产业协会、雷风影视、海洋 cms、梦雨 cms、快看 CMS、ZBlogger 社区、Kong Inc.、zzzcms 和 MyuCMS。

本周，CNVD 发布了《关于 Android-gif-Drawable 开源库存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5257

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、华为技术有限公司、深信服科技股份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、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、远江盛邦（北京）网络安全科技股份

有限公司、内蒙古奥创科技有限公司、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、任子行网络技术股份有限公司、北京君信安科技有限公司、广州锦行网络科技有限公司、河南信安世纪科技有限公司、杭州海康威视数字技术股份有限公司、北京智游网安科技有限公司、新疆海狼科技有限公司、广州蕴辰网络科技有限公司、国家互联网应急中心、北京圣博润高新技术股份有限公司、北京信联科汇科技有限公司、雷石安全实验室、厦门靠谱云股份有限公司及其他个人白帽子向 CNVD 提交了 8002 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 7044 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）	5742	5742
斗象科技（漏洞盒子）	1065	1065
上海交大	237	237
哈尔滨安天科技集团股份有限公司	278	0
北京天融信网络安全技术有限公司	277	11
北京神州绿盟科技有限公司	103	2
华为技术有限公司	79	0
深信服科技股份有限公司	73	0
恒安嘉新(北京)科技股份公司	61	0
新华三技术有限公司	50	0
厦门服云信息科技有限公司	45	1
北京启明星辰信息安全技术有限公司	41	0
中新网络信息安全股份有限公司	33	33
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	10	10
西安四叶草信息技术有限公司	5	5

北京知道创宇信息技术股份有限公司	4	0
南京联成科技发展股份有限公司	1	1
国瑞数码零点实验室	111	111
南京众智维信息科技有限公司	105	105
山东新潮信息技术有限公司	66	66
远江盛邦（北京）网络安全科技股份有限公司	63	63
内蒙古奥创科技有限公司	38	38
北京华云安信息技术有限公司	30	30
山东云天安全技术有限公司	18	18
任子行网络技术股份有限公司	10	10
北京君信安科技有限公司	8	8
广州锦行网络科技有限公司	6	6
河南信安世纪科技有限公司	5	5
杭州海康威视数字技术股份有限公司	3	3
北京智游网安科技有限公司	2	2
新疆海狼科技有限公司	2	2
广州蕴辰网络科技有限公司	2	2
国家互联网应急中心	1	1
北京圣博润高新技术股份有限公司	1	1
北京信联科汇科技有限公司	1	1
雷石安全实验室	1	1
厦门靠谱云股份有限公司	1	1

CNCERT 西藏分中心	7	7
CNCERT 贵州分中心	4	4
CNCERT 宁夏分中心	4	4
CNCERT 吉林分中心	1	1
个人	377	377
报送总计	9118	8002

本周漏洞按类型和厂商统计

本周，CNVD 收录了 478 个漏洞。应用程序 219 个，操作系统 142 个，WEB 应用 79 个，网络设备（交换机、路由器等网络端设备）22 个，安全产品 10 个，智能设备（物联网终端设备）漏洞 5 个，数据库 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	219
操作系统	142
WEB 应用	79
网络设备（交换机、路由器等网络端设备）	22
安全产品	10
智能设备（物联网终端设备）漏洞	5
数据库	1

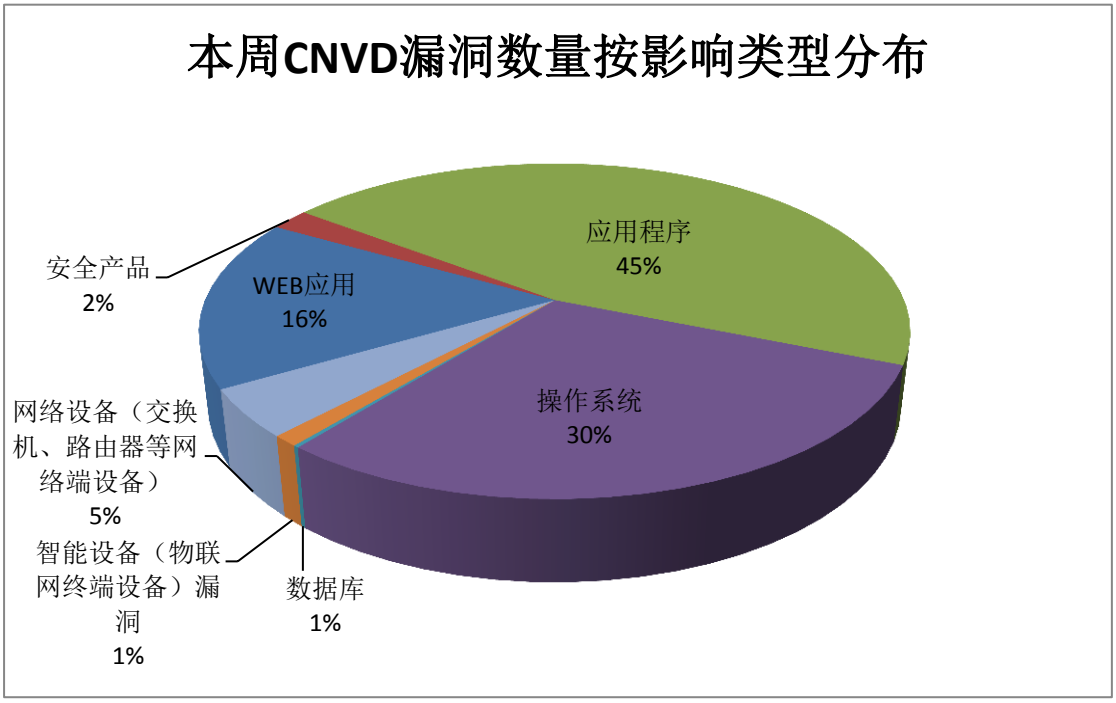

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Oracle、Linux 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	Google	97	20%
2	Oracle	91	19%
3	Linux	45	9%
4	WordPress	35	7%
5	Microsoft	19	4%
6	FusionPBX	18	4%
7	IBM	14	3%
8	CloudBees	7	2%
9	Mozilla	6	1%
10	其他	146	31%

本周行业漏洞收录情况

本周，CNVD 收录了 4 个电信行业漏洞，77 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“FusionPBX Call Center Queue Module 命令注入漏洞、Google Android 提权漏洞（CNVD-2019-37964）”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/

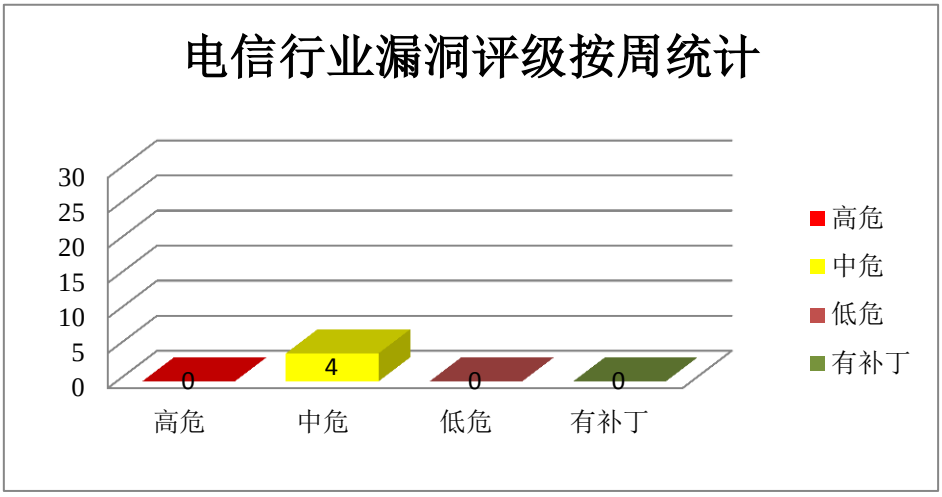

图 3 电信行业漏洞统计

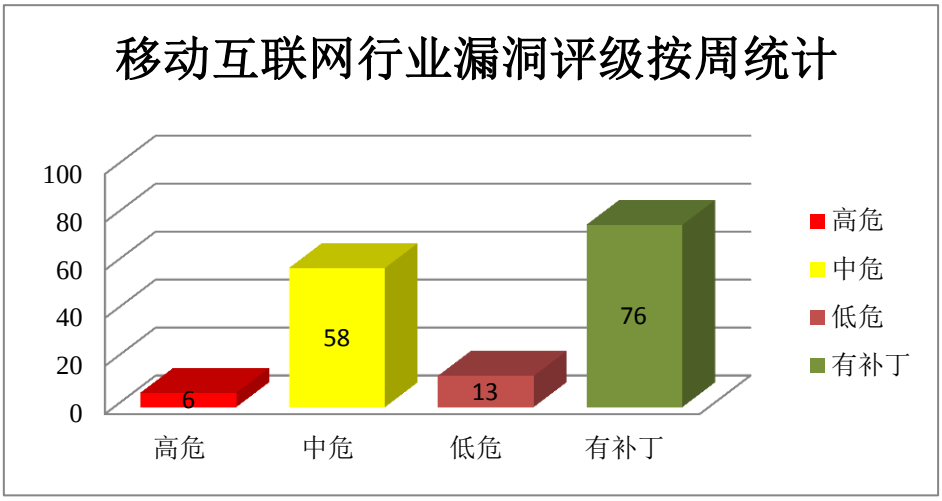

图 4 移动互联网行业漏洞统计

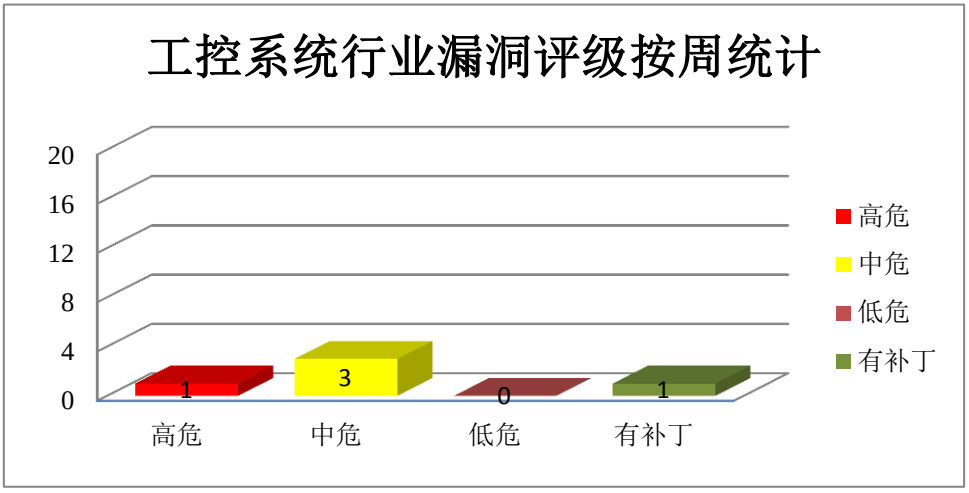

图 5 工控系统行业漏洞统计

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

Google Chrome 是一款 Web 浏览器。Android 是美国 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，该产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 远程代码执行漏洞（CNVD-2019-37947、CNVD-2019-37953、CNVD-2019-37954）、Google Android 提权漏洞（CNVD-2019-37971）、Google Chrome 权限许可和访问控制问题漏洞（CNVD-2019-38243、CNVD-2019-38246、CNVD-2019-38251）、Google Chrome 代码注入漏洞。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-2019-37947

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37953

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37954

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37971

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38243

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38246

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38244

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38251

2、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会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，攻击者可利用漏洞执行任意命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Linux kernel 内存破坏漏洞（CNVD-2019-37726）、Linux Kernel 空指针解引用漏洞（CNVD-2019-38263、CNVD-2019-38266）、Linux kernel 输入验证错误漏洞（CNVD-2019-38515）、Linux kernel 缓冲区溢出漏洞（CNVD-2019-38516、CNVD-2019-38519）、Linux kernel 本地特权升级漏洞、Linux kernel 越界访问漏洞（CNVD-2019-38518）。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-2019-37726

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38263

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38266

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38515

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38516

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38518

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38519

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38530

3、WordPress 产品安全漏洞

WordPress 是 WordPress 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。wps-hide-login 是使用在其中的一个隐藏登录插件。syndication-links 是使用在其中的一个页面链接添加插件。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客户端代码、进行服务器端请求伪造攻击等。

CNVD 收录的相关漏洞包括：WordPress 跨站请求伪造漏洞（CNVD-2019-37377）、WordPress 输入验证错误漏洞（NVD-C-2019-153344）、WordPress 跨站脚本漏洞（CNVD-2019-37380）、WordPress 信息泄露漏洞（CNVD-2019-37381）、WordPress 服务器端请求伪造漏洞（CNVD-2019-37383、CNVD-2019-37382）、WordPress syndication-links 插件跨站脚本漏洞、WordPress wps-hide-login 插件跨站请求伪造漏洞。其中“WordPress 服务器端请求伪造漏洞（CNVD-2019-37383、CNVD-2019-37382）”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-2019-37377

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37379

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37380

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37381

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37382

http://www.cnvd.org.cn/flaw/show/CNVD-2019-37383

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38058

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38061

4、Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Windows Jet Database Engine 是其中的一个数据库引擎。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Jet Database Engine 远程代码执行漏洞（CNVD-2019-38614、CNVD-2019-38615、CNVD-2019-38616、CNVD-2019-38617、CNVD-2019-38618、CNVD-2019-38619、CNVD-2019-38620、CNVD-2019-38621）。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-2019-38614

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38615

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38616

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38617

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38618

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38619

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38620

http://www.cnvd.org.cn/flaw/show/CNVD-2019-38621

5、SageMath Sage Cell Server 操作系统命令注入漏洞

SageMath Sage Cell Server 是一款 Cell 服务器，它能够提供将 Sage 计算嵌入到网页中的方法。本周，SageMath Sage Cell Server 被披露存在操作系统命令注入漏洞。攻击者可利用该漏洞在底层操作系统上执行任意命令。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：https://www.cnvd.org.cn/flaw/show/CNVD-2019-37729

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-2019-37731	Sonatype Nexus Repository Manager 远程代码执行漏洞（CNVD-2019-37731）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.sonatype.com/hc/en-us/articles/360036132453-CVE-2019-16530-Nexus-Repository-Manager-2-3-and-Nexus-IQ-Server-Remote-Code-Execution-2019-09-19
CNVD-2019-37876	FusionPBX Call Center Queue Module 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://github.com/fusionpbx/fusionpbx/commit/2f9e591a4034c3aea70185dcab837946096449bf
CNVD-2019-37880	Citrix Systems NetScaler Gateway 和 Citrix Application Delivery Controller 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.citrix.com/article/CTX261055
CNVD-2019-37884	GNU libidn2 缓冲区错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/libidn/libidn2/commit/e4d1558aa2c1c04a05066ee8600f37603890ba8c

CNVD-2019-38063	Mozilla Firefox 和 Mozilla Firefox ESR 资源管理错误漏洞（CNVD-2019-38063）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2019-33/
CNVD-2019-38467	YouPHPTube Encoder 操作系统命令注入漏洞	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.youphptube.com/
CNVD-2019-38469	Chunghwa Telecom HiNet GPON 命令执行漏洞	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.cht.com.tw
CNVD-2019-38471	Chunghwa Telecom HiNet GPON 存取控制缺陷漏洞	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.cht.com.tw
CNVD-2019-38477	Broadcom CA Network Flow Analysis 默认凭据漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://techdocs.broadcom.com/us/product-content/recommended-reading/security-notices/new-security-notice-ca-20190930-01-security-notice-for-ca-network-flow-analysis.html
CNVD-2019-38482	Mozilla Firefox 权限提升漏洞（CNVD-2019-38482）	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.mozilla.org/en-US/security/advisories/mfsa2019-34/

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码。此外，Linux、WordPress、Microsoft 等多款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，导致拒绝服务等。另外，SageMath Sage Cell Server 操作系统命令注入漏洞。攻击者可利用该漏洞在底层操作系统上执行任意命令。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、Apache Solr 基于 Velocity 模板远程命令执行漏洞

验证描述

Apache Solr 是美国阿帕奇（Apache）软件基金会的一款基于 Lucene（一款全文搜索引擎）的搜索服务器。该产品支持层面搜索、垂直搜索、高亮显示搜索结果等。

Apache Solr 基于 Velocity 模板存在远程命令执行漏洞。该漏洞是由于 Velocity 模板存在注入所致。攻击者可利用漏洞访问 Solr 服务器上 Core 名称，先把 params.resource.loader.enabled 设置为 true（就可加载指定资源），在服务器执行命令。

验证信息

POC 链接：https://gist.githubusercontent.com/s00py/a1ba36a3689fa13759ff910e179fc133/raw/fae5e663ffac0e3996fd9dbb89438310719d347a/

参考链接： https://www.cnvd.org.cn/flaw/show/CNVD-2019-38290

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. Avast 杀毒软件中 5000 美元的 XSS 漏洞

Avast 杀毒软件之所以会提取 SSID，是因为它有监控流量的功能，在用户连接到某个新的网络中，就会向用户发出警报。例如下图就是当用户连接上 My Hotspot 无线网络时的警报。此时 SSID 出现在窗口的中央，这也就是 XSS 注入的位置。虽然 SSID 一般有 32 个字符的长度限制，但是我们还是可以通过其他研究员的智慧进行攻击（Brute Logic 和 S0md3v）。

参考链接：https://nosec.org/home/detail/3118.html

2. 微软承认新 BUG：使用持久性内存的设备会出现启动缓慢问题

在近日更新的官方支持文档中，微软承认了存在于 Windows 操作系统中的一个 BUG，不过所幸的是普通消费者并没有受到负面影响。在支持文档中，微软承认使用持久性内存（Persistent Memory）的部分设备可能会出现启动缓慢的情况。

参考链接：https://www.dbsec.cn/blog/article/5327.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