国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 01 月 07 日-2019 年 01 月 13 日 **2019 年第 2 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 225 个，其中高危漏洞 68 个、中危漏洞 139 个、低危漏洞 18 个。漏洞平均分值为 5.94。本周收录的漏洞中，涉及 0day 漏洞 134 个（占 60%），其中互联网上出现“WhatsApp 远程内存破坏漏洞、inxedu 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 1475 个，与上周（1496 个）环比下降 1%。

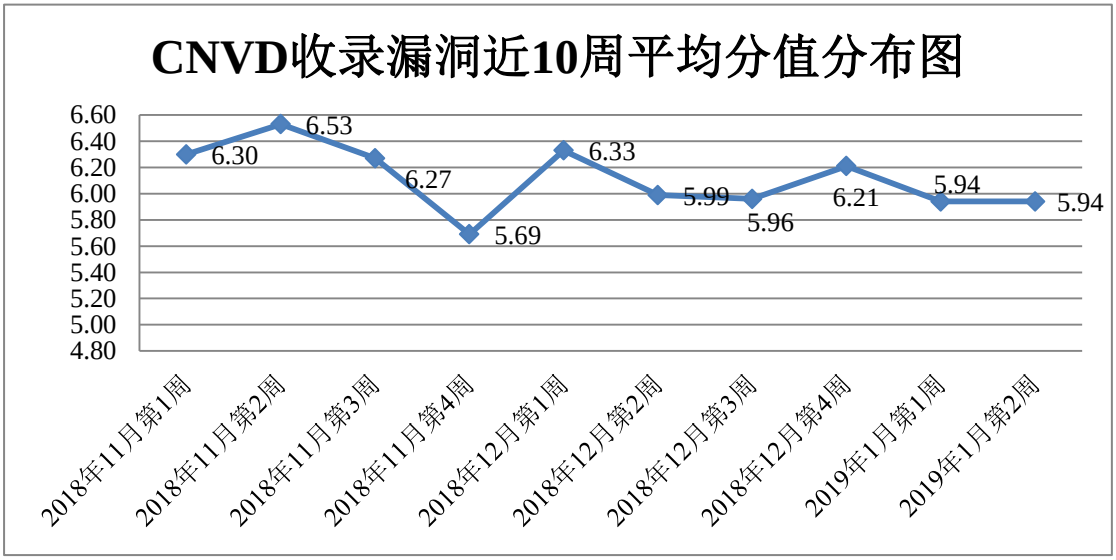

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向银行、保险、能源等重要行业单位通报漏洞事件 23 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 301 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 90 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 20 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：

北京元恒时代科技有限公司、洪湖尔创网联信息技术有限公司、中国建材检验认证集团股份有限公司、中国国机重工集团有限公司、西安佰联网络技术有限公司、网际傲游北京科技有限公司、成都康菲顿特网络科技有限公司、江苏鑫跃科技有限公司、深一科技集团有限公司、广州瀚德网络科技有限公司、灵宝简好网络科技有限公司、北京五指互联科技有限公司、上海卓卓网络科技有限公司、武汉贝云网络科技有限公司、上海斐讯数据通信技术有限公司、成都砺寒软件有限公司、中国中医科学院、Cisco、XYCMS、Schoolcms。

本周，CNVD 发布了《Microsoft 发布 2018 年 11 月安全更新》、《Microsoft 发布 2018 年 12 月安全更新》、《Microsoft 发布 2019 年 01 月安全更新》和《关于 ThinkPHP 5.0.x 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。

http://www.cnvd.org.cn/webinfo/show/4849

http://www.cnvd.org.cn/webinfo/show/4851

http://www.cnvd.org.cn/webinfo/show/4853

http://www.cnvd.org.cn/webinfo/show/4855

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、华为技术有限公司、深信服科技股份有限公司、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。中新网络信息安全股份有限公司、天津市国瑞数码安全系统股份有限公司、安徽锋刃信息科技有限公司、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、远江盛邦（北京）网络安全科技股份有限公司、北京国舜科技股份有限公司、北京圣博润高新技术股份有限公司、广州竞远安全技术股份有限公司、北京山石网科信息技术有限公司、河南信安世纪科技有限公司、上海零盾网络科技有限公司、四川博全科技有限公司及其他个人白帽子向 CNVD 提交了 1475 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 926 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）	475	475
360 网神（补天平台）	451	451

北京天融信网络安全技术有限公司	219	20
哈尔滨安天科技集团股份有限公司	143	0
华为技术有限公司	136	0
深信服科技股份有限公司	67	0
新华三技术有限公司	66	0
中国电信集团系统集成有限责任公司	51	0
北京神州绿盟科技有限公司	47	0
恒安嘉新(北京)科技股份公司	46	0
北京启明星辰信息安全技术有限公司	37	0
北京数字观星科技有限公司	14	0
北京知道创宇信息技术有限公司	5	4
中新网络信息安全股份有限公司	75	75
天津市国瑞数码安全系统股份有限公司	66	66
安徽锋刃信息科技有限公司	52	52
山东云天安全技术有限公司	31	31
任子行网络技术股份有限公司	18	18
远江盛邦（北京）网络安全科技股份有限公司	13	13
北京国舜科技股份有限公司	10	10
北京圣博润高新技术股份有限公司	7	7
广州竞远安全技术股份有限公司	5	5
北京山石网科信息技术有限公司	4	4
河南信安世纪科技有限公司	1	1

上海零盾网络科技有限公司	1	1
四川博全科技有限公司	1	1
CNCERT 上海分中心	6	6
CNCERT 新疆分中心	5	5
CNCERT 吉林分中心	4	4
CNCERT 宁夏分中心	3	3
CNCERT 河北分中心	1	1
个人	222	222
报送总计	2282	1475

本周漏洞按类型和厂商统计

本周，CNVD 收录了 225 个漏洞。应用程序漏洞 130 个，WEB 应用漏洞 57 个，操作系统漏洞 24 个，网络设备漏洞 14 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	130
WEB 应用漏洞	57
操作系统漏洞	24
网络设备漏洞	14

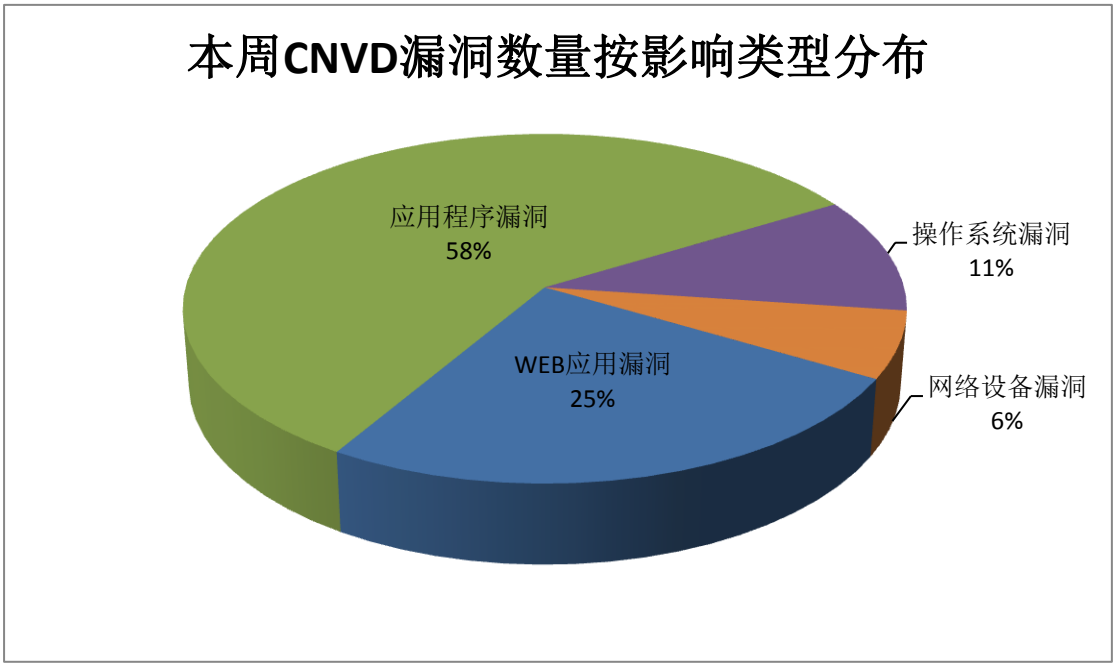

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、TerraMaster、libming 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	Microsoft	24	11%
2	TerraMaster	14	6%
3	libming	9	4%
4	Radare	9	4%
5	UCMS	9	4%
6	DouPHP	8	4%
7	BUFFALO	7	3%
8	SIEMENS	7	3%
9	FreeRDP	6	3%
10	其他	132	58%

本周行业漏洞收录情况

本周，CNVD 收录了 1 个电信行业漏洞，6 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，“SIEMENS CP1604 和 CP1616 设备拒绝服务漏洞、Siemens SIMATIC S7-1500 CPU 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/

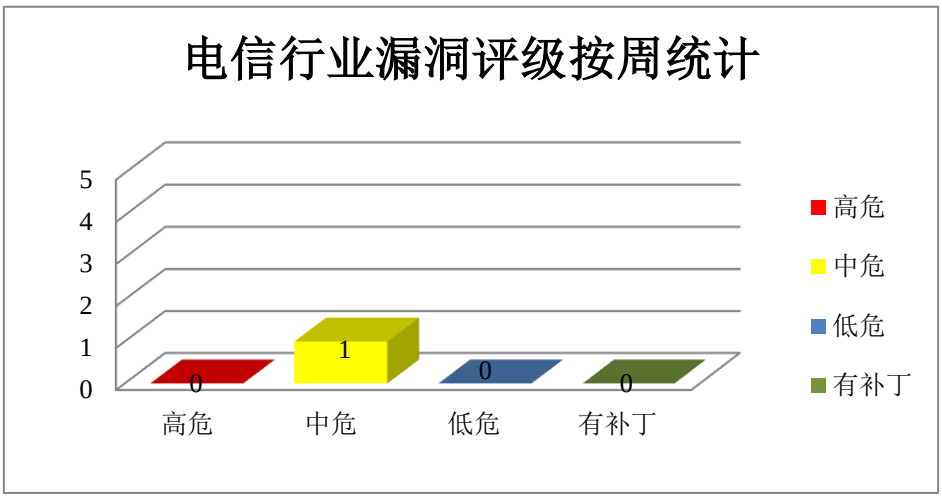

图 3 电信行业漏洞统计

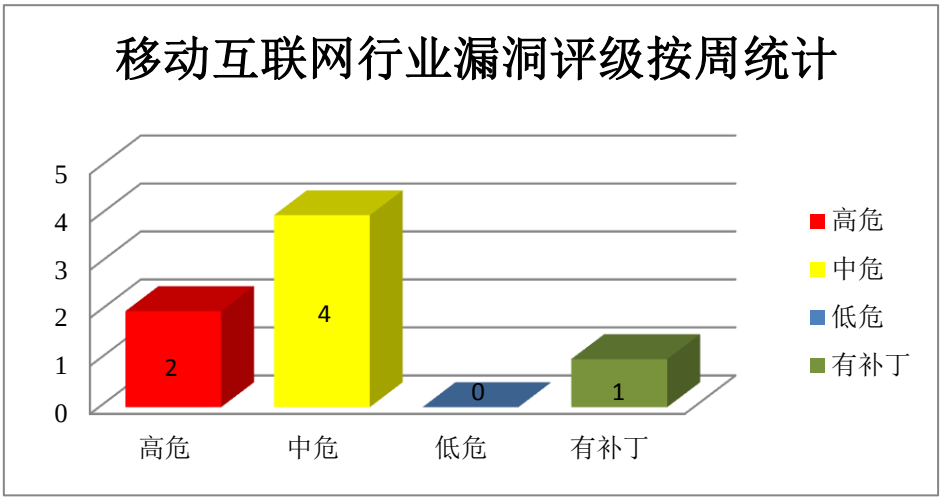

图 4 移动互联网行业漏洞统计

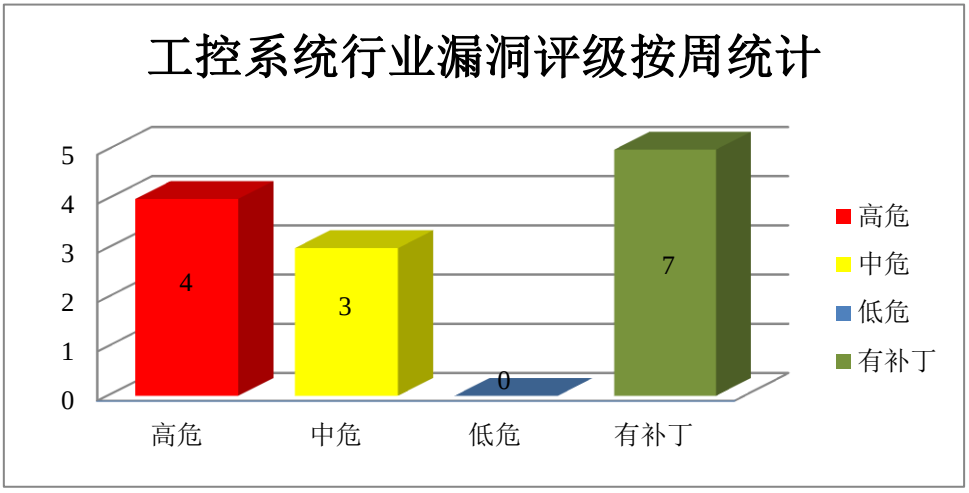

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Word 是一款文字处理软件。Microsoft Excel 是一款电子表格处理软件。Microsoft PowerPoint 是一个文档演示工具。Microsoft Exchange Server 是一套电子邮件服务程序，它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。Microsoft Windows 10、Windows Server 2019 等都是美国微软（Microsoft）公司发布的一系列操作系统。Windows Hyper-V 是其中的一个虚拟化产品，支持在 Windows 中创建虚拟机。Edge 是其中的一个系统附带的浏览器。ChakraCore 是使用在 Edge 的一个开源的 JavaScript 引擎的核心部分，也可作为单独的 JavaScript 引擎使用。本周，上述产品被披露存在远程执行代码漏洞，攻击者可利用漏洞在系统用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Word 远程代码执行漏洞（CNVD-2019-00630）、Microsoft Excel 远程代码执行漏洞（CNVD-2019-00635）、Microsoft Chakra Scripting Engine 远程内存破坏漏洞、Microsoft Windows DHCP Client 远程代码执行漏洞、Microsoft PowerPoint 远程代码执行漏洞（CNVD-2019-00804）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2019-00958、CNVD-2019-00962）、Microsoft Exchange Server 远程执行代码漏洞。上述漏洞的综合评级为为“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-2019-00630

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00635

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00760

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00764

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00804

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00958

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00962

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00967

2、SIEMENS 产品安全漏洞

SIEMENS SIMATIC S7-1500 是模块化结构的控制器系列产品。SIEMENS SIMATIC S7-300 CPU 是一款用于制造行业的模块化通用控制器。SIEMENS CP1604 是用于将 PCI-104 系统连接到 PROFINET IO。SIEMENS CP1616 是一种创新产品，安装在 PC 中，用于 PROFINET 通讯。SIEMENS 是凭借电气化、自动化和数字化领域的创新，在发电和输配电、基础设施、工业自动化、驱动和软件等领域为客户提供解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：SIEMENS SIMATIC S7-1500 CPU 拒绝服务漏洞（CNVD-2019-00984、CNVD-2019-00985）、SIEMENS SIMATIC S7-300 CPU 拒绝服务漏洞（CNVD-2019-00986）、SIEMENS CP1604 和 CP1616 设备拒绝服务漏洞、SIEMENS CP1604 和 CP1616 设备跨站脚本漏洞、SIEMENS CP1604 和 CP1616 设备跨站请求伪造漏洞、SIEMENS ICAM A8000 系列拒绝服务漏洞。其中，“SIEMENS SIMATIC S7-1500 CPU 拒绝服务漏洞（CNVD-2019-00984、CNVD-2019-00985）、SIEMENS SIMATIC S7-300 CPU 拒绝服务漏洞（CNVD-2019-00986）、SIEMENS CP1604 和 CP1616 设备拒绝服务漏洞”的综合评级为为“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-2019-00984

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00985

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00986

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00987

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00988

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00989

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00990

3、Radare 产品安全漏洞

radare2 是一套用来处理二进制文件的库和工具。本周，上述产品被披露存在缓冲区溢出和拒绝服务漏洞，攻击者可利用漏洞造成拒绝服务（应用程序崩溃）。

CNVD 收录的相关漏洞包括：radare2 'parseOperands'函数栈缓冲区溢出漏洞、radare2 'armass_assemble'函数堆缓冲区溢出漏洞、radare2 'r_bin_dyldcache_extract'函数堆缓冲区溢出漏洞、radare2 'assemble'函数堆缓冲区溢出漏洞、radare2 'getToken'函数拒绝服务漏洞、radare2 'parseOperand'函数拒绝服务漏洞、radare2 'parseOperand'函数栈缓冲区溢出漏洞、radare2 'core_anal_bytes'函数堆缓冲区溢出漏洞。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-2019-00779

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00780

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00781

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00782

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00786

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00783

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00784

http://www.cnvd.org.cn/flaw/show/CNVD-2019-00787

4、TerraMaster 品安全漏洞

TerraMaster TOS 是一套基于 Linux 平台开发的存储服务器专用操作系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞执行 SQL 查询、泄露敏感信息、执行系统命令。

CNVD 收录的相关漏洞包括：TerraMaster TOS 目录遍历漏洞、TerraMaster TOS 跨站脚本漏洞（CNVD-2019-00660）、TerraMaster TOS 系统命令注入漏洞（CNVD-2019-00661、CNVD-2019-00663、CNVD-2019-00665）、TerraMaster TOS 会话固定漏洞、TerraMaster TOS 会话泄露漏洞、TerraMaster TOS SQL 注入漏洞。其中，“TerraMaster TOS 系统命令注入漏洞（CNVD-2019-00661、CNVD-2019-00663、CNVD-2019-00665）、TerraMaster TOS SQL 注入漏洞”的综合评级为为“高危”。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-2019-00659
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00660
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00661
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00663
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00664
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00667
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00665
http://www.cnvd.org.cn/flaw/show/CNVD-2019-00669

5、August Connect 信息泄露漏洞

August Connect 是一款用于支持 Wi-Fi 和智能锁连接的网桥设备。本周，August Connect 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取家用 Wi-Fi 凭证。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-2019-00774

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-2019-00559	IBM API Connect 信息泄露漏洞（CNVD-2019-00559）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www-01.ibm.com/support/docview.wss?uid=ibm10793601
CNVD-2019-00638	libgit2 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://libgit2.org/
CNVD-2019-00649	FreeRDP NTLM Authentication 模块越界读取漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/FreeRDP/FreeRDP/c

			ommit/2ee663f39dc8dac3d9988e847db19b2d7e3ac8c6
CNVD-2019-00656	KioWare Server 权限提升漏洞	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.kioware.com/
CNVD-2019-00725	Dolibarr SQL 注入漏洞（CNVD-2019-00725）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/Dolibarr/dolibarr/commit/2b088a73c121a52e006c0d76ea4da7ffeb7b4f4a
CNVD-2019-00763	Microsoft Edge 远程内存破坏漏洞（CNVD-2019-00763）	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0565
CNVD-2019-00777	Vtiger CRM 文件上传 PHP 代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://code.vtiger.com/vtiger/vtigercrm/commit/52fc2fb520ddc55949c2fbedaabd61ddd0109375
CNVD-2019-00821	PRTG Network Monitor 文件包含漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.paessler.com/prtg/history/stable#18.2.40.1683
CNVD-2019-00830	Centreon 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://github.com/centreon/centreon/pull/6627/commits/c817c34dad99234ab3fbe70ad2a40edd2d2ce62d
CNVD-2019-00975	hsweb 跨站请求伪造漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/hs-web/hsweb-framework/commit/40929e9b0d336a26281a5ed2e0e721d54dd8d2f2

小结：本周，Microsoft 被披露存在多个漏洞，攻击者可利用漏洞在系统用户的上下文中执行任意代码。此外，SIEMENS、Radare、TerraMaster 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行 SQL 查询、泄露敏感信息、执行系统命令或发起拒绝服务攻击等。另外，August Connect 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取家用 Wi-Fi 凭证。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、WhatsApp 远程内存破坏漏洞

验证描述

WhatsApp 是一款目前可供 iPhone 手机、Android 手机、Windows Phone 手机、WhatsApp Messenger、Symbian 手机和黑莓手机用户使用的、用于智能手机之间通讯的应用程序。

WhatsApp 2.18.31 版本存在内存破坏漏洞，攻击者可利用漏洞使受影响的应用程序崩溃,拒绝服务合法用户正常使用。

验证信息

POC 链接：https://www.exploit-db.com/exploits/44629

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-00628

信息提供者

杭州安恒信息技术股份有限公司

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. 某通用交易所框架组合型严重漏洞

近日 BUGX 平台收到一个基于 POSCMS 开发的交易所高危漏洞。此漏洞利用 XSS（Cross Site Scripting）+CSRF（Cross-site request forgery）组合型通用漏洞，漏洞可把普通会员提升为交易所管理员权限，登录管理后台进行敏感操作。已导致多家交易所中招。

参考链接：https://www.freebuf.com/vuls/193960.html

2. ThinkPHP 5.0.*远程代码执行漏洞

Thinkphp 5.0.*存在远程代码执行漏洞。攻击者可以利用漏洞实现任意代码执行等高危操作。该漏洞出现在处理请求的类中。攻击者可以控制类的属性及类方法的调用。目前网上已有该远程代码执行漏洞的 POC，请尽快升级更新官方的补丁。

参考链接：https://www.easyaq.com/news/1173155130.shtml

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