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 25 日-2019 年 12 月 01 日 **2019 年第 48 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 402 个，其中高危漏洞 91 个、中危漏洞 276 个、低危漏洞 35 个。漏洞平均分值为 5.59。本周收录的漏洞中，涉及 0day 漏洞 125 个（占 31%），其中互联网上出现“vBulletin 远程命令执行漏洞（CNVD-2019-42750）、Jobberbase 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 1893 个，与上周（2044 个）环比减少 7%。

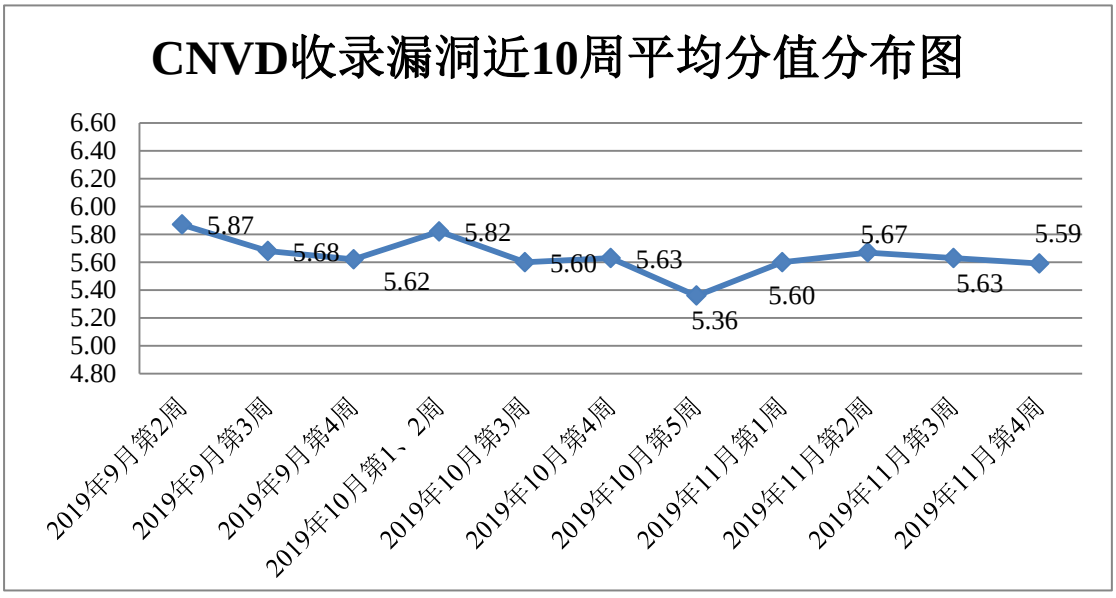

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 8 起，向基础电信企业通报漏洞事件 12 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 187 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 42 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 11 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：

网际傲游(北京)科技有限公司、西安泽瑞通信有限公司、洛阳云业信息科技有限公司、北京东土科技股份有限公司、湖南壹拾捌号网络技术有限公司、衡水金航计算机科技有限公司、台达电子企业管理(上海)有限公司、十堰八五科技有限公司、山西企凝信息科技有限公司、四川迅睿云软件开发有限公司、友讯电子设备（上海）有限公司、广州购啊购科技有限公司、海南易而优科技有限公司、北京灵州网络技术有限公司、北京良精志诚科技有限责任公司、睿谷信息科技有限公司、北京点威创奇教育科技发展有限公司、深圳市乙辰科技股份有限公司、海南赞赞网络科技有限公司、北京畅聊天下科技股份有限公司、北京米尔伟业科技有限公司、北京云易优科技有限公司、北京新锦成数据科技有限公司、上海泛微网络科技股份有限公司、长沙海商网络技术有限公司、启明星工作室、中国消费者协会、奥壹科技（OE）团队、Newbee-mall、ZrLog、UQCMS、XnSoft 和 Digi International Inc。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、北京铭图天成信息技术有限公司、杭州迪普科技股份有限公司、内蒙古奥创科技有限公司、杭州海康威视数字技术股份有限公司、山东新潮信息技术有限公司、北京华云安信息技术有限公司、南京众智维信息科技有限公司、河南信安世纪科技有限公司、山东云天安全技术有限公司、上海端御信息科技有限公司、新疆海狼科技有限公司、北京圣博润高新技术股份有限公司、山东华鲁科技发展股份有限公司、江苏保旺达软件技术有限公司、国家互联网应急中心、广州蕴辰网络科技有限公司、河南灵创电子科技有限公司 、北京君信安科技有限公司、山石网科通信技术股份有限公司、北京智游网安科技有限公司及其他个人白帽子向 CNVD 提交了 1893 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 1164 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）	560	560
上海交大	355	355

斗象科技（漏洞盒子）	249	249
哈尔滨安天科技集团股份有限公司	235	0
北京天融信网络安全技术有限公司	220	2
华为技术有限公司	139	0
北京启明星辰信息安全技术有限公司	121	26
厦门服云信息科技有限公司	83	0
北京神州绿盟科技有限公司	79	0
深信服科技股份有限公司	67	0
北京知道创宇信息技术股份有限公司	59	58
恒安嘉新(北京)科技股份公司	53	0
新华三技术有限公司	38	0
中国电信集团系统集成有限责任公司	37	37
北京数字观星科技有限公司	20	0
南京联成科技发展股份有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	75	75
国瑞数码零点实验室	50	50
北京铭图天成信息技术有限公司	41	41
杭州迪普科技股份有限公司	21	5
内蒙古奥创科技有限公司	19	19
杭州海康威视数字技术股份有限公司	16	16
山东新潮信息技术有限公司	14	14
北京华云安信息技术有限公司	10	10

南京众智维信息科技有限公司	8	8
河南信安世纪科技有限公司	6	6
山东云天安全技术有限公司	5	5
上海端御信息科技有限公司	5	5
新疆海狼科技有限公司	4	4
北京圣博润高新技术股份有限公司	4	4
山东华鲁科技发展股份有限公司	3	3
江苏保旺达软件技术有限公司	2	2
国家互联网应急中心	2	2
广州蕴辰网络科技有限公司	2	2
河南灵创电子科技有限公司	2	2
北京君信安科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京智游网安科技有限公司	1	1
CNCERT 天津分中心	4	4
CNCERT 新疆分中心	1	1
个人	322	322
报送总计	2937	1893

本周漏洞按类型和厂商统计

本周，CNVD 收录了 402 个漏洞。应用程序 304 个，操作系统 35 个，网络设备（交换机、路由器等网络端设备）30 个，WEB 应用 24 个，智能设备（物联网终端设备）5 个，安全产品 4 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	304
操作系统	35
网络设备（交换机、路由器等网络端设备）	30
WEB 应用	24
智能设备（物联网终端设备）漏洞	5
安全产品	4

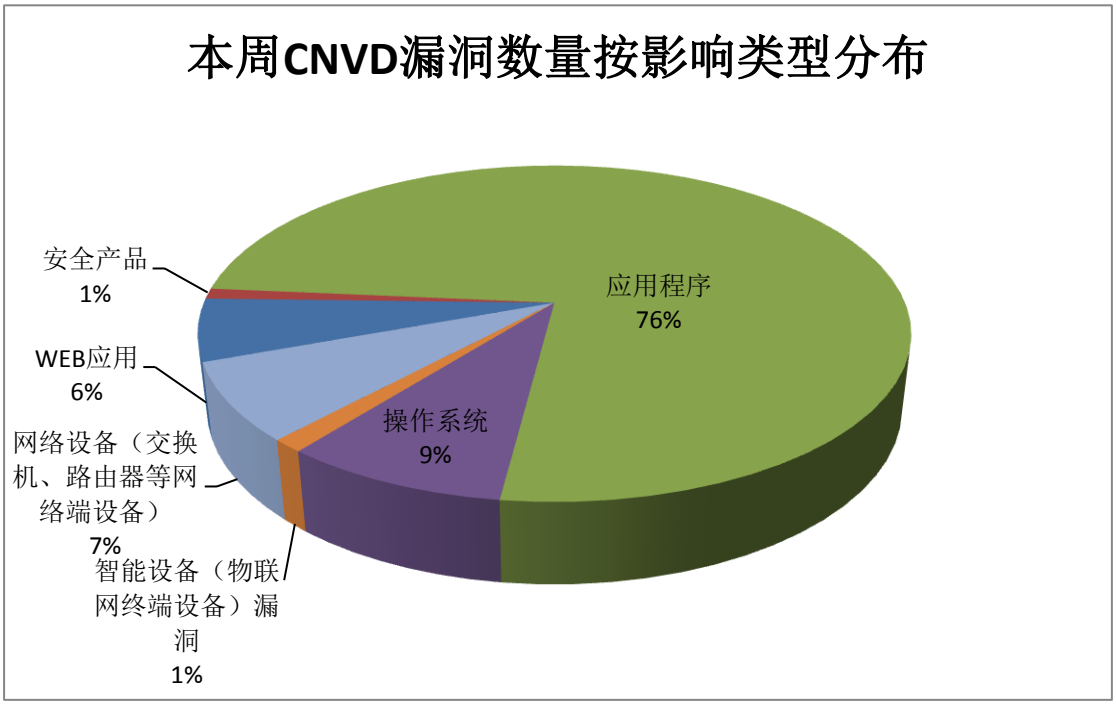

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Intel、CloudBees、Microsoft 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	Intel	37	9%
2	CloudBees	36	9%
3	Microsoft	21	6%
4	GitLab	20	5%
5	Linux	17	4%
6	Google	16	4%
7	WordPress	12	3%
8	Centreon	11	3%
9	Technicolor	10	2%
10	其他	309	55%

本周行业漏洞收录情况

本周，CNVD 收录了 17 个电信行业漏洞，6 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，“Cisco IOS XE 拒绝服务漏洞（CNVD-2019-42591）、Grandstream UCM6204 命令注入漏洞、ABB Power Generation Information Manager (PGIM) and Plant Connect 安全验证绕过漏洞、3S-Smart Software Solutions CODESYS 缓冲区错误漏洞、多款 Huawei 产品不恰当授权漏洞”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/

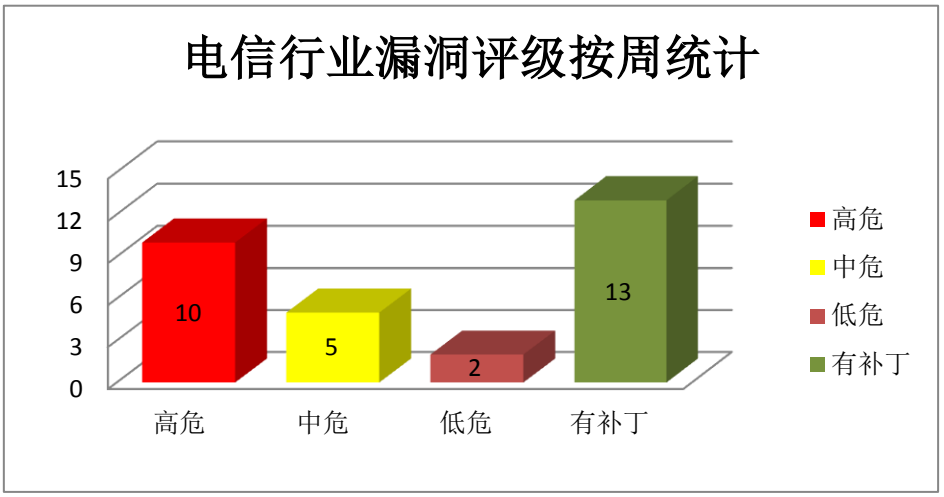

图 3 电信行业漏洞统计

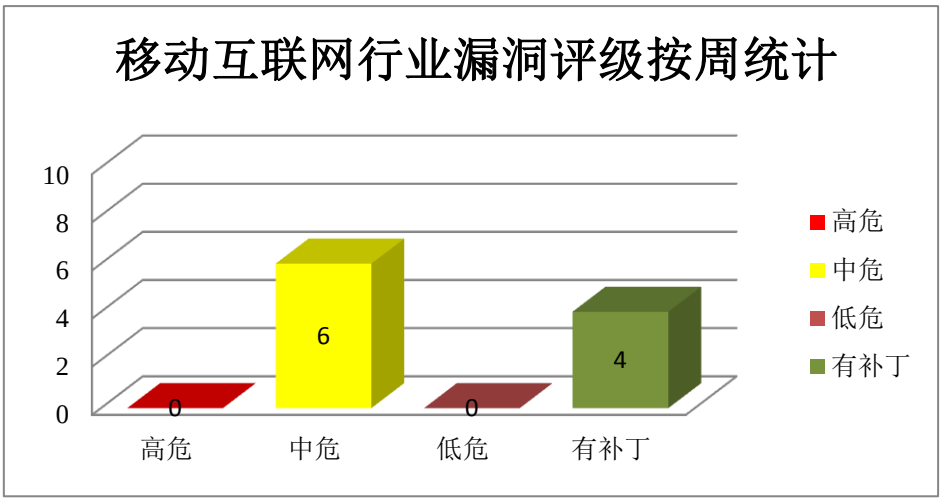

图 4 移动互联网行业漏洞统计

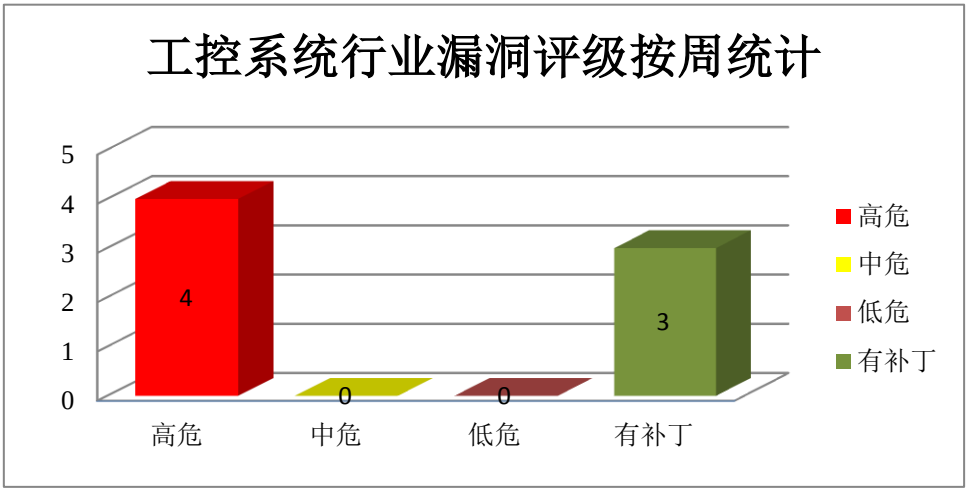

图 5 工控系统行业漏洞统计

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、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 Hyper-V 是其中的一个虚拟化产品，支持在 Windows 中创建虚拟机。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致主机服务器崩溃等。

CNVD 收录的相关漏洞包括：Microsoft Windows Hyper-V 拒绝服务漏洞（CNVD-2019-42609、CNVD-2019-42610、CNVD-C-2019-194159、CNVD-C-2019-194158）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2019-42611、CNVD-2019-42612、CNVD-2019-42608）、Microsoft Edge 脚本引擎内存破坏漏洞（CNVD-2019-42802）。其中，“Microsoft Windows Hyper-V 远程执行代码漏洞（CNVD-2019-42608、CNVD-2019-42611、CNVD-2019-42612）、Microsoft Edge 脚本引擎内存破坏漏洞（CNVD-2019-42802）”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-2019-42607

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42608

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42609

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42610

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42611

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42612

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42613

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42802

2、Cisco 产品安全漏洞

Cisco MDS 9000 Series Multilayer Switches 等都是美国思科（Cisco）公司的产品。Cisco MDS 9000 Series Multilayer Switches 是一款 MDS 9000 系列多层交换机。Cisco Nexus 7000 Series Switches 是一款 7000 系列交换机。Cisco Nexus 7700 Series Switches 是一款 7700 系列交换机。Cisco Nexus 3000 Series Switches 是一款 3000 系列交换机。Cisco Nexus 3500 Platform Switches 是一款 3500 系列平台交换机。Cisco Nexus 3600 Platform Switches 是一款 3600 系列平台交换机。Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。Cisco IOS XE 是一套为其网络设备开发的操作系统。Cisco Integrated Management Controller (IMC) Supervisor 是一套机架式服务器集中管理系统。Cisco UCS Director 是一套私有云基础架构即服务（IaaS）的异构平台。Cisco UCS Director Express for Big Data 是一套针对大数据集群的基础架构统一管理平台。Cisco Unified Communications Manager（CUCM，Unified CM，CallManager）是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。该组件提供了一种可扩展、可分布和高可用的企业 IP 电话呼叫处理解决方案。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访问权限，执行任意命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco NX-OS Software CLI 命令注入漏洞、Cisco IOS XE 拒绝服务漏洞（CNVD-2019-42591）、Cisco Integrated Management Controller Supervisor、Cisco UCS Director 和 Cisco UCS Director Express for Big Data 信任管理问题漏洞、Cisco Integrated Management Controller Supervisor、Cisco UCS Director 和 Cisco UCS Director Express for Big Data 输入验证错误漏洞、Cisco Integrated Management Controller Supervisor、Cisco UCS Director 和 Cisco UCS Director Express for Big Data 身份验证绕过漏洞、Cisco NX-OS 和 Cisco IOS XE 数据伪造问题漏洞、Cisco NX-OS Software 操作系统命令注入漏洞、Cisco Unified Communications Manager SQL 注入漏洞（CNVD-2019-42752）。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-2019-42590

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42591

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42592

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42593

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42594

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42596

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42597

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42752

3、Intel 产品安全漏洞

Intel Converged Security and Management Engine（CSME）和 Intel TXE 等都是美国英特尔（Intel）公司的产品。Intel Converged Security and Management Engine 是一款安全管理引擎。Intel TXE 是一款使用在 CPU（中央处理器）中具有硬件验证功能的信任执行引擎。Intel Active Management Technology（AMT）是一套以硬件为基础的计算机远程主动管理技术软件。Intel Graphics Driver 是 Intel 显卡驱动程序。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，导致拒绝服务。

CNVD 收录的相关漏洞包括：Intel Graphics Driver 内存破坏漏洞（CNVD-2019-42247）、Intel Graphics Driver 代码问题漏洞、Intel Active Management Technology 权限提升漏洞（CNVD-2019-42601、CNVD-2019-42606、CNVD-2019-42598）、Intel Converged Security and Management Engine 和 Intel TXE 缓冲区溢出漏洞、Intel Converged Security and Management Engine 权限提升漏洞、Intel Active Management Technology 信息泄露漏洞。其中，除“Intel Graphics Driver 代码问题漏洞、Intel Active Management Technology 权限提升漏洞（CNVD-2019-42601、CNVD-2019-42598）”外的综合评级为“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-2019-42247

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42248

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42601

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42598

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42600

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42603

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42606

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42605

4、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。contact-form-multi 是使用在其中的一个联系表单自定义插件。custom-admin-page 是使用在其中的一个自定义后台管理页面插件。contact-form-7-sms-addon 是使用在其中的一个短消息提醒插件。wp-support-plus-responsive-ticket-system 是使用在其中的一个票务系统插件。plugmatter-optin-feature-box-lite 是使用在其中的一个功能列表插件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行客户端代码等。

CNVD 收录的相关漏洞包括：WordPress contact-form-multi 插件跨站脚本漏洞、WordPress custom-admin-page 插件跨站脚本漏洞、WordPress contact-form-7-sms-addon 插件跨站脚本漏洞、WordPress wp-support-plus-responsive-ticket-system 插件路径遍历漏洞、

WordPress wp-support-plus-responsive-ticket-system 插件信息泄露漏洞、WordPress wp-support-plus-responsive-ticket-system 插件 SQL 注入漏洞、WordPress plugmatter-optin-feature-box-lite 插件 SQL 注入漏洞（CNVD-2019-42838）、WordPress download-plugins-dashboard 插件跨站脚本漏洞。其中，“WordPress wp-support-plus-responsive-ticket-system 插件 SQL 注入漏洞、WordPress plugmatter-optin-feature-box-lite 插件 SQL 注入漏洞（CNVD-2019-42838）”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-2019-42037

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42039

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42038

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42043

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42044

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42045

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42838

http://www.cnvd.org.cn/flaw/show/CNVD-2019-42840

5、Linux kernel 内存破坏漏洞（CNVD-2019-42788）

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，Linux kernel 被披露存在内存破坏漏洞。攻击者可利用该漏洞创建原始套接字。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-2019-42788

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-2019-42244	Centreon SQL 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/centreon/centreon/pull/7862
CNVD-2019-42377	Eclipse Jetty 缓冲区溢出漏洞	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.eclipse.org/jetty/
CNVD-2019-42388	Linux kernel 空指针解引用漏洞（CNVD-2019-42388）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.195
CNVD-2019-42426	多款 Huawei 产品不恰当授权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20191113-01-homerouter-cn
CNVD-2019-42428	ABB Power Generation Information Manager (PGIM) and Plant Connect 安全验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.abb.com
CNVD-2019-42751	3S-Smart Software Solutions CODESYS 缓冲区错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://customers.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-10_CDS-68341.pdf
CNVD-2019-42756	Google Chrome 资源管理错误漏洞（CNVD-2019-42756）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2019/07/stable-channel-update-for-desktop.html
CNVD-2019-42771	NVIDIA Windows GPU Display Driver DirectX 驱动缓冲区溢出漏洞（CNVD-2019-42771）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://nvidia.custhelp.com/app/answers/detail/a_id/4841/
CNVD-2019-42779	Apache Commons Beanutils 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://issues.apache.org/jira/browse/BEANUTILS-520
CNVD-2019-43040	GitLab 访问控制错误漏洞（CNVD-2019-43040）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://about.gitlab.com/2019/03/14/gitlab-11-8-2-released/

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致主机服务器崩溃等。此外，Cisco、Intel、WordPress 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，执行任意命令，提升权限，导致拒绝服务等。另外，Linux kernel 被披露存在内存破坏漏洞。攻击者可利用该漏洞创建原始套接字。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、vBulletin 远程命令执行漏洞（CNVD-2019-42750）

验证描述

vBulletin 是美国 InternetBrands 和 vBulletinSolutions 公司的一款基于 PHP 和 MySQ

L 的开源 Web 论坛程序。

vBulletin 5.x 版本至 5.5.4 版本中存在远程命令执行漏洞，攻击者可借助‘widgetConfig[code]’参数利用该漏洞执行命令。

验证信息

POC 链接：https://packetstormsecurity.com/files/154648/vBulletin-5.x-Pre-Auth-Remote-Code-Execution.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2019-42750

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. 首都网警发布预警通报：OPENSSL 加密组件存在重大风险隐患

首都网警发布网络安全预警通报称，据国家网络与信息安全信息通报中心监测发现，互联网 SSL 协议实现组件 OPENSSL 部分版本存在重大安全隐患，可能导致信息泄露等风险

参考链接：https://t.cj.sina.com.cn/articles/view/2833534593/a8e44e8102000kpte

2. Google RCS 可与 iMessage 媲美 但目前仍是一场安全噩梦

安全研究人员指出，RCS 不仅没有像 iMessage 一样做到端到端加密，且事实证明其在用户隐私和数据安全性上留下了巨大的隐患。SRLabs 研究人员向 Motherboard 解释称：RCS 的第一个问题，就是在安全措施方面缺乏统一性。用户数据存在被泄露的风险，因为某些市场中可利用 RCS 来显示文本消息和呼叫内容、或查明用户的位置。

参考链接：https://www.cnbeta.com/articles/tech/916453.htm

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