国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 11 月 16 日-2020 年 11 月 22 日　　2020 年第 47 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 477 个，其中高危漏洞 109 个、中危漏洞 245 个、低危漏洞 123 个。漏洞平均分值为 5.34。本周收录的漏洞中，涉及 0day 漏洞 206 个（占 43%），其中互联网上出现“Ghisler Total Commander 权限提升漏洞、Symphony CMS 跨站脚本漏洞（CNVD-2020-63998）”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 4995 个，与上周（4094 个）环比增加 22%。

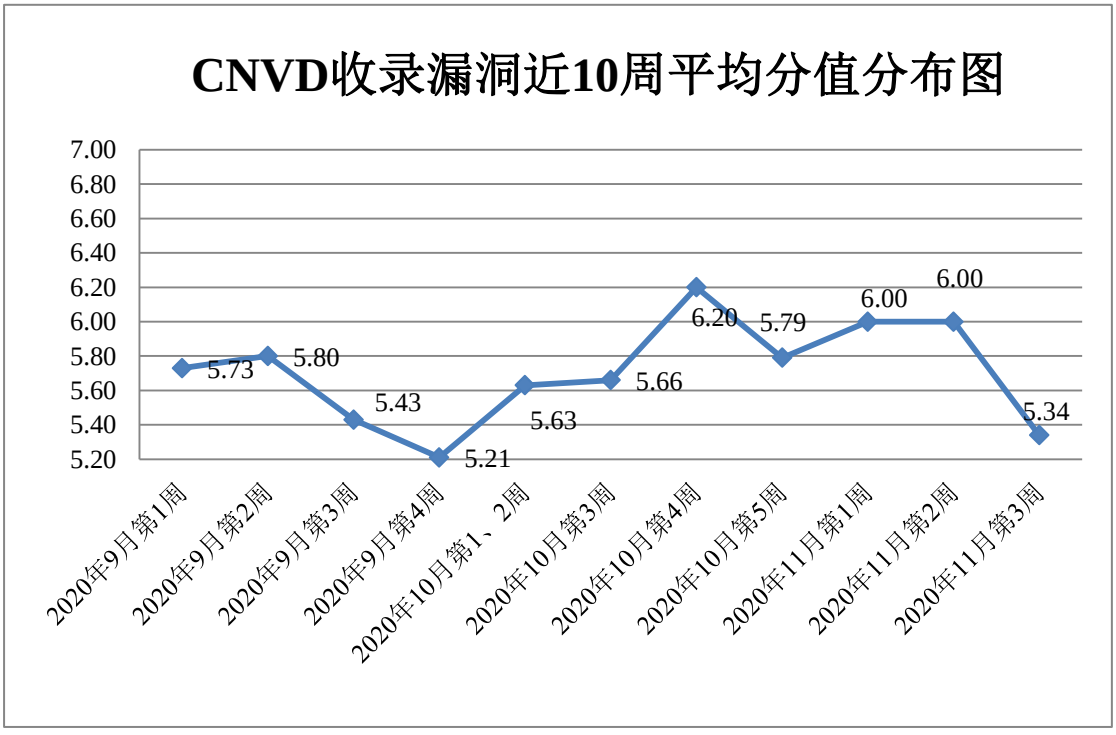

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 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 276 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 80 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 23 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：

浙江大华技术股份有限公司、零视技术(上海)有限公司、长沙友点软件科技有限公司、遵义欣腾达信息技术有限公司、北京小米科技有限责任公司、深圳市圆梦云科技有限公司、鹏为软件股份有限公司、北京中创视讯科技有限公司、漳州盾灵网络科技有限公司、深圳国裕网络科技有限公司、北京致远互联软件股份有限公司、南京晨曦网络科技有限公司、深圳市科迈通讯技术有限公司、辽宁华睿科技有限公司、杭州铭师堂教育科技发展有限公司、成都科来软件有限公司、北京金方时代科技有限公司、石家庄捷搜网络科技有限公司、福建福昕软件开发股份有限公司、珠海云麦科技有限公司、驰通集团股份有限公司、瑞芯微电子股份有限公司、微软(中国)有限公司、苏州思杰马克丁软件有限公司、深圳市精浦科技有限公司、杭州美迪网络技术有限公司、烟台艾睿光电科技有限公司、河北南昊高新技术开发有限公司、重庆米未科技有限公司、上海步科自动化股份有限公司、上海展盟网络科技有限公司、北京因酷时代科技有限公司、施耐德电气(中国)有限公司、北京中成科信科技发展有限公司、四川思途智旅软件有限公司、南通点酷网络科技有限公司、淮南市银泰软件科技有限公司、哈尔滨伟成科技有限公司、北京云梦网络科技有限公司、北京文华在线信息技术有限公司、深圳市吉祥腾达科技有限公司、新开普电子股份有限公司、上海报业集团新闻报社、网展科技、若依、米酷资源网、狂雨小说 cms、MyuCMS、BEESCMS、Victor CMS、ZZCMS 和 SEACMS。

本周，CNVD 发布了《CNVD 关于开放厂商用户自主获取和更新漏洞信息功能的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5839

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、北京神州绿盟科技有限公司、北京天融信网络安全技术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、山东云天安全技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京天地和兴科技有限公司、河南灵创电子科技有限公司 、山东新潮信息技术有限公司、南京众智维信息科技有限公司、杭州海康威视数字技术股份有限公司、杭州迪普科技股份有限公司、内蒙古奥创科技有限公司、北京零零信安科技有限公司、山东华鲁科技发展股份有限公司、广

州市蓝爵计算机科技有限公司、吉林谛听信息技术有限公司、星云博创科技有限公司、广西等保安全测评有限公司、河南信安世纪科技有限公司、江苏保旺达软件技术有限公司、北京机沃科技有限公司、联想全球安全实验室、北京长亭科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、上海观安信息技术股份有限公司、安徽长泰信息安全服务有限公司、山东道普测评技术有限公司、深圳市魔方安全科技有限公司、四川哨兵信息科技有限公司、上海犀点意象网络科技有限公司、北京智游网安科技有限公司、广西塔易信息技术有限公司、广州安亿信软件科技有限公司、新疆海狼科技有限公司、中移（杭州）信息技术有限公司及其他个人白帽子向 CNVD 提交了 4995 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 3015 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）	2005	2005
上海交大	619	619
奇安信网神（补天平台）	391	391
阿里云计算有限公司	320	0
哈尔滨安天科技集团股份有限公司	219	0
华为技术有限公司	162	0
北京神州绿盟科技有限公司	133	19
北京天融信网络安全技术有限公司	126	12
新华三技术有限公司	122	0
中国电信股份有限公司网络安全产品运营中心	60	0
北京启明星辰信息安全技术有限公司	51	0
北京数字观星科技有限公司	34	0
深信服科技股份有限公司	20	0
西安四叶草信息技术有限公司	19	19

北京知道创宇信息技术股份有限公司	6	0
中新网络信息安全股份有限公司	2	2
国瑞数码零点实验室	179	179
山东云天安全技术有限公司	45	45
远江盛邦（北京）网络安全科技股份有限公司	45	45
北京天地和兴科技有限公司	34	34
河南灵创电子科技有限公司	31	31
山东新潮信息技术有限公司	28	28
南京众智维信息科技有限公司	24	24
杭州海康威视数字技术股份有限公司	16	16
杭州迪普科技股份有限公司	14	0
内蒙古奥创科技有限公司	14	14
北京零零信安科技有限公司	13	13
山东华鲁科技发展股份有限公司	13	13
广州市蓝爵计算机科技有限公司	9	9
吉林谛听信息技术有限公司	9	9
星云博创科技有限公司	9	9
广西等保安全测评有限公司	7	7
河南信安世纪科技有限公司	7	7
江苏保旺达软件技术有限公司	7	7
北京机沃科技有限公司	6	6
联想全球安全实验室	6	6

北京长亭科技有限公司	5	5
北京云科安信科技有限公司（Seraph 安全实验室）	4	4
上海观安信息技术股份有限公司	4	4
安徽长泰信息安全服务有限公司	3	3
山东道普测评技术有限公司	3	3
深圳市魔方安全科技有限公司	3	3
四川哨兵信息科技有限公司	3	3
上海犀点意象网络科技有限公司	1	1
北京智游网安科技有限公司	1	1
广西塔易信息技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
新疆海狼科技有限公司	1	1
中移（杭州）信息技术有限公司	1	1
CNCERT 辽宁分中心	8	8
CNCERT 山西分中心	7	7
CNCERT 西藏分中心	3	3
CNCERT 贵州分中心	1	1
个人	1376	1376
报送总计	6231	4995

本周漏洞按类型和厂商统计

本周，CNVD 收录了 477 个漏洞。应用程序 276 个，WEB 应用 147 个，操作系统 18 个，网络设备（交换机、路由器等网络端设备）15 个，数据库 9 个，智能设备（物联网终端设备）8 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	276
WEB 应用	147
操作系统	18
网络设备（交换机、路由器等网络端设备）	15
数据库	9
智能设备（物联网终端设备）	8
安全产品	4

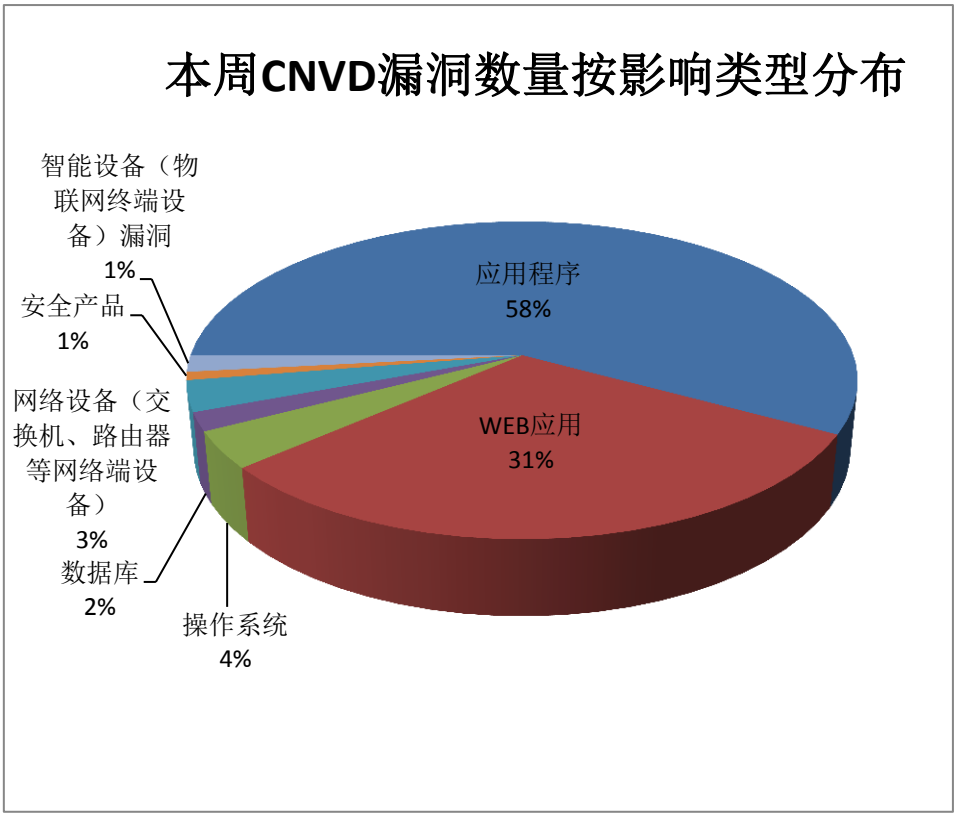

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Hancom、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	Microsoft	46	10%
2	Hancom	40	8%
3	Google	30	6%
4	IBM	18	4%
5	Oracle	15	3%

6	GitLab	10	2%
7	WordPress	10	2%
8	用友网络科技股份有限公司	10	2%
9	BEESCMS	8	2%
10	其他	290	61%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，6 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“ASUS TM-AC1900 任意命令执行漏洞”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/

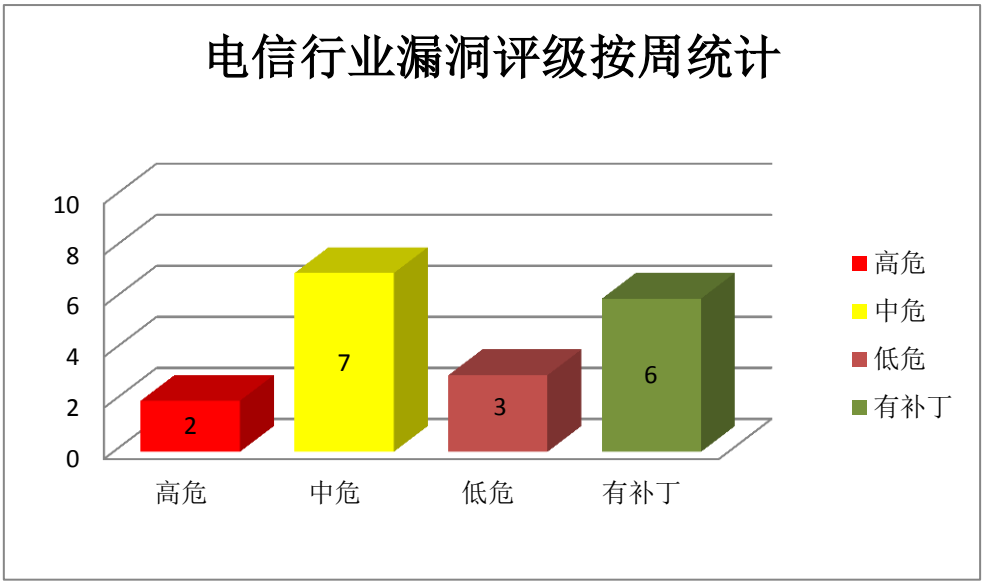

图 3 电信行业漏洞统计

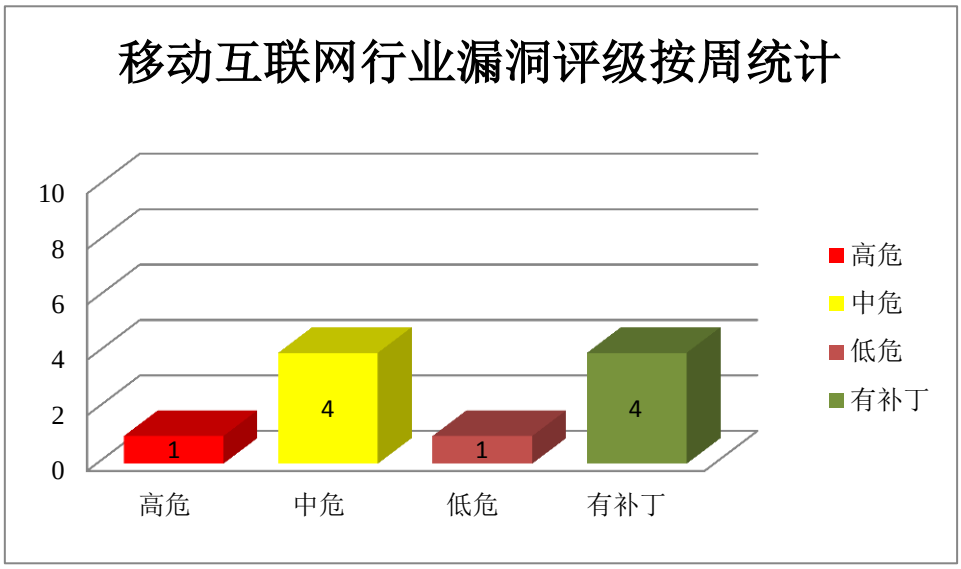

图 4 移动互联网行业漏洞统计

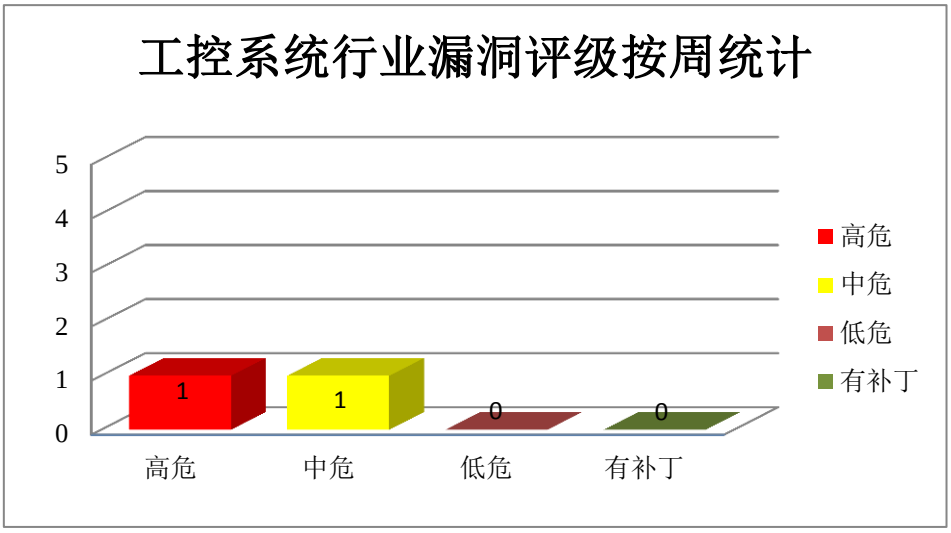

图 5 工控系统行业漏洞统计

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 SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。Azure Sphere 是一个安全的高级应用程序平台，具有用于联网设备的内置通信和安全功能。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资源 ID、SAS 令牌、用户属性和其他敏感信息，执行任意代码，触发拒绝服务等。

CNVD 收录的相关漏洞包括：Microsoft SharePoint 远程代码执行漏洞（CNVD-2020-63731、CNVD-2020-63730、CNVD-2020-63733）、Microsoft Azure Sphere 拒绝服务漏洞、Microsoft Azure Sphere 篡改漏洞、Microsoft Azure Sphere 权限提升漏洞（CNVD-

2020-63391、CNVD-2020-63390）、Microsoft Azure Sphere 信息泄露漏洞。其中，“Microsoft SharePoint 远程代码执行漏洞（CNVD-2020-63731、CNVD-2020-63730、CNVD-2020-63733）”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-63731
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63730
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63733
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63387
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63386
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63391
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63390
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63389

2、Google 产品安全漏洞

Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具。本周，上述产品被披露存在多个漏洞，攻击者可利用通过精心制作的 WebRTC 流利用堆破坏，通过一个 HTML 页面绕过站点隔离，利用堆破坏，执行一个沙箱逃脱等。

CNVD 收录的相关漏洞包括：Google Chrome 释放后重用漏洞（CNVD-2020-63264、CNVD-2020-63268、CNVD-2020-63271、CNVD-2020-63270、CNVD-2020-63269、CNVD-2020-63273、CNVD-2020-63272）、Google Chrome 整数溢出漏洞（CNVD-2020-63266）。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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-63264
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63268
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63266
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63271
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63270
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63269
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63273
https://www.cnvd.org.cn/flaw/show/CNVD-2020-63272

3、IBM 产品安全漏洞

IBM UrbanCode Deploy（UCD）是美国 IBM 公司的一套应用自动化部署工具。IBM Sterling B2B Integrator 是美国 IBM 公司的一套集成了重要的 B2B 流程、交易和关系的软件。IBM Business Automation Workflow 是美国 IBM 公司的一套工作流程自动化解决方案。IBM Sterling File Gateway 是美国 IBM 公司的一款文件传输集中式管理网关产品。IBM Sterling B2B Integrator 是美国 IBM 公司的一套集成了重要的 B2B 流程、交易和关

系的软件。IBM App Connect Enterprise 是美国 IBM 公司的一个操作系统。IBM Sterling B2B Integrator 是一个交易引擎，是一套根据您的业务需求运行您定义和管理的流程的组件。IBM Sterling File Gateway 是一款用于在内部和外部合作伙伴之间传输文件的应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发送专门编写的 SQL 语句，这些语句允许攻击者查看、添加、修改或删除后端数据库中的信息，在 Web UI 中嵌入任意 JavaScript 代码，从而改变预期的功能，从而可能导致可信会话中的凭据泄露，劫持受害者的点击动作，并可能对受害者进行进一步的攻击等。

CNVD 收录的相关漏洞包括：IBM UrbanCode Deploy 安全绕过漏洞（CNVD-2020-63484）、IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2020-63942）、IBM Business Automation Workflow 跨站脚本漏洞（CNVD-2020-63941）、IBM Sterling File Gateway SQL 注入漏洞（CNVD-2020-63940）、IBM Sterling B2B Integrator 授权问题漏洞、IBM App Connect Enterprise 点击劫持漏洞、IBM Sterling B2B Integrator Standard Edition 信息泄露漏洞（CNVD-2020-63967）、IBM Sterling File Gateway 信息泄露漏洞（CNVD-2020-63969）。其中，“IBM Sterling B2B Integrator 授权问题漏洞”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-63484

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63942

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63941

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63940

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63939

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63943

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63967

https://www.cnvd.org.cn/flaw/show/CNVD-2020-63969

4、Oracle 产品安全漏洞

Oracle FLEXCUBE Direct Banking 使银行可基于人口统计学和细分市场提供量身定制的、基于门户的丰富在线客户体验。Oracle CRM Technical Foundation 是美国甲骨文（Oracle）公司的一个 CRM 应用程序开发和部署的基础组件。Oracle FLEXCUBE Universal Banking 是一项实时、在线、全面的全球核心银行业务方案，涵盖零售、企业及投资银行业务。Oracle PeopleSoft Enterprise PeopleTools 是美国甲骨文（Oracle）公司的一个支持转变企业管理。Oracle Banking Corporate Lending 是美国甲骨文（Oracle）公司的一个银行贷款管理组件。Oracle Banking Payments 是一个完整的支付处理解决方案。Oracle Hospitality Suite8 是美国甲骨文（Oracle）公司的一个应用于酒店管理的数字化解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未经授权访问关键数据或完全访问所有 Oracle FLEXCUBE Direct Banking 可访问的数据，未经授权

访问关键数据或完全访问所有 Oracle FLEXCUBE Universal Banking 可访问的数据等。

CNVD 收录的相关漏洞包括：Oracle FLEXCUBE Direct Banking 信息泄露漏洞（CNVD-2020-64252）、Oracle FLEXCUBE Direct Banking 信息泄露漏洞、Oracle CRM Technical Foundation 未授权访问漏洞、Oracle FLEXCUBE Universal Banking 信息泄露漏洞（CNVD-2020-64251）、Oracle PeopleSoft Enterprise PeopleTools 授权问题漏洞、Oracle Banking Corporate Lending 信息泄露漏洞、Oracle Banking Payments 信息泄露漏洞（CNVD-2020-64254）、Oracle Hospitality Suite8 WebConnect 未授权访问漏洞。其中，“Oracle FLEXCUBE Direct Banking 信息泄露漏洞（CNVD-2020-64252）、Oracle FLEXCUBE Direct Banking 信息泄露漏洞、Oracle CRM Technical Foundation 未授权访问漏洞”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-64252
https://www.cnvd.org.cn/flaw/show/CNVD-2020-64253
https://www.cnvd.org.cn/flaw/show/CNVD-2020-64261
https://www.cnvd.org.cn/flaw/show/CNVD-2020-64251
https://www.cnvd.org.cn/flaw/show/CNVD-2020-64256
https://www.cnvd.org.cn/flaw/show/CNVD-2020-64255
https://www.cnvd.org.cn/flaw/show/CNVD-2020-64254
https://www.cnvd.org.cn/flaw/show/CNVD-2020-64259

5、Linux kernel perf_event_parse_addr_filter()代码问题漏洞

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，Linux kernel perf_event_parse_addr_filter()被披露存在代码问题漏洞。攻击者可利用该漏洞可以通过 perf_event_parse_addr_filter()来创建内存泄漏，从而触发拒绝服务。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-2020-64300

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-2020-63628	F5 BIG-IP 跨站脚本漏洞（CNVD-2020-63628）	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.qualcomm.com/company/product-security/bulletins/november-2020-security-bulletin
CNVD-2020-63627	Moxa MXView 本地权限提升漏洞	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.moxa.com/en/support/support/security-advisory/mxview-series-network-management-software-vulnerabilities
CNVD-2020-63975	XStream 远程代码执行漏洞（CNVD-2020-63975）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/x-stream/xstream/commit/0fec095d534126931c99fd38e9c6d41f5c685c1a
CNVD-2020-63980	ASUS TM-AC1900 任意命令执行漏洞	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.asus.com/sg/Networking/RT-AC88U/HelpDesk_BIOS/
CNVD-2020-63997	Crafter CMS 动态管理代码资源控制不当漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2020080102
CNVD-2020-63999	Juniper Networks Junos OS Evolved 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://kb.juniper.net/InfoCenter/index?page=content&id=JSA11063
CNVD-2020-64265	Nagios XI 和 Nagios 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.nagios.com/downloads/nagios-xi/change-log/
CNVD-2020-64299	Atlassian Jira gajira-create 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/atlassian/gajira-comment/security/advisories/GHSA-hj6w-pm28-h8hf
CNVD-2020-64301	Mozilla Firefox MCallGetProperty 代码问题漏洞	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.mozilla.org/en-US/security/advisories/mfsa2020-49/
CNVD-2020-64563	Drupal 远程代码执行漏洞（CNVD-2020-64563）	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.drupal.org/sa-core-2020-012

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞获取资源 ID、SAS 令牌、用户属性和其他敏感信息，执行任意代码，触发拒绝服务等。此外，Google、IBM、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 WebRTC 流利用堆破坏，发送专门编写的 SQL 语句，这些语句允许攻击者查看、添加、

修改或删除后端数据库中的信息，未经授权访问关键数据或完全访问所有 Oracle FLEXCUBE Direct Banking 可访问的数据等。另外，Linux kernel perf_event_parse_addr_filter()被披露存在代码问题漏洞。攻击者可利用该漏洞可以通过 perf_event_parse_addr_filter()来创建内存泄漏，从而触发拒绝服务。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、Symphony CMS 跨站脚本漏洞（CNVD-2020-63998）

验证描述

Symphony CMS 是一款基于 PHP + MySQL 的、使用 XML 和 XSLT 作为骨干的开源内容管理系统。

Symphony CMS 3.0.0 存在跨站脚本漏洞。远程攻击者可通过 eventsevent.publish_article.php 利用该漏洞将任意 Web 脚本或 HTML 注入到 fields['body']参数中。

验证信息

POC 链接：https://www.exploit-db.com/exploits/48773

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-63998

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. 微软发布 Pluton 处理器 为 Windows PC 提供全新安全功能

微软与 AMD、英特尔和高通公司合作开发了新的 Pluton 安全处理器。这款新的安全处理器将使攻击者访问系统的难度大大增加，它还将提高微软防范物理攻击的能力，防止凭证和加密密钥被盗，并提供从软件漏洞中恢复的能力。

参考链接：https://www.cnbeta.com/articles/tech/1054715.htm

2. Chrome 87 发布，具有性能提升和安全修复

11 月 17 日，Google 发布了 Chrome 87，其中更新了许多性能改进，包括安全修复和新功能添加。Windows，Mac 和 Linux 桌面用户可以通过转到设置->帮助->关于 Google Chrome 升级到 Chrome 87 。然后，浏览器将自动检查新更新并在可用时进行安装。

参考链接：https://www.bleepingcomputer.com/news/google/chrome-87-released-with-performance-boost-and-security-fixes/

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