国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 09 月 07 日-2020 年 09 月 13 日　　2020 年第 37 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 395 个，其中高危漏洞 142 个、中危漏洞 194 个、低危漏洞 59 个。漏洞平均分值为 5.80。本周收录的漏洞中，涉及 0day 漏洞 188 个（占 48%），其中互联网上出现“WordPress Click To Top 插件存储型跨站脚本漏洞、Joomla! J2 Store 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 4632 个，与上周（3165 个）环比增加 46%。

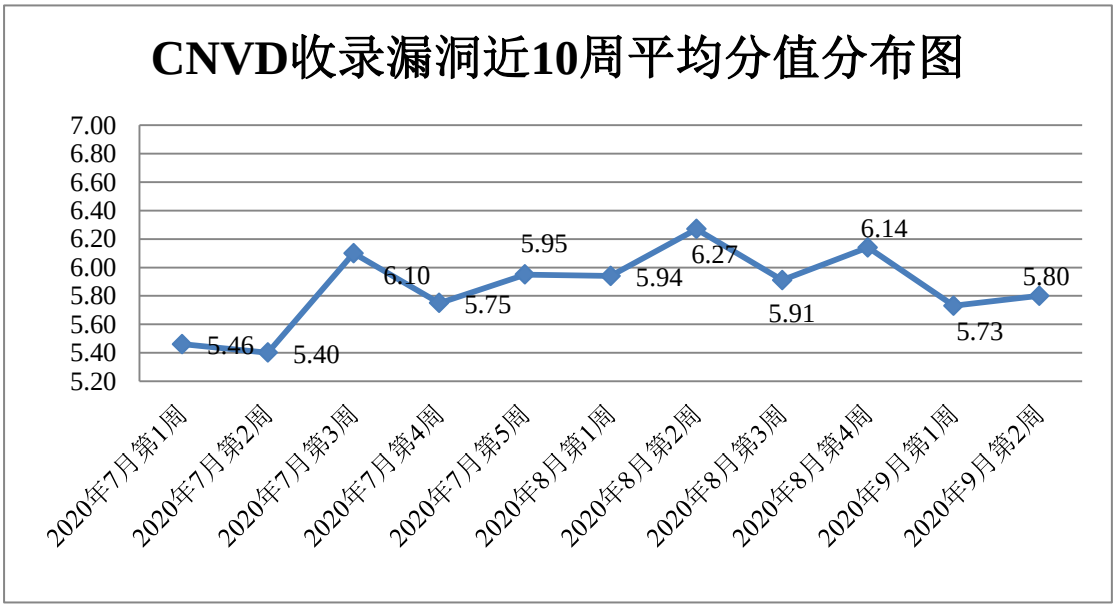

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 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 335 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 108 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 53 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：

海南易而优科技有限公司、北京通达信科科技有限公司、用友网络科技股份有限公司、淄博闪灵网络科技有限公司、保定市互动企业营销策划有限公司、润申信息科技（上海）有限公司、安徽九五信息科技有限公司、桂林启航软件开发有限公司、瑞芯微电子股份有限公司、研华科技（中国）有限公司、北京玛格泰克科技发展有限公司 、南京友博网络科技有限公司、深圳市迅雷网文化有限公司、苏州托普斯网络科技有限公司、长沙米拓信息技术有限公司、合肥明信软件技术有限公司、哈尔滨巨耀网络科技有限公司、成都新线加科技有限公司、互联网域名系统北京市工程研究中心有限公司、福建福昕软件开发股份有限公司、深圳市汇川技术股份有限公司、厦门小皮网络有限公司、深圳幻美网络科技有限公司、上海白帽子信息科技有限公司、云南华企优享网络科技有限公司、武汉灯火阑珊科技有限公司、北京爱奇艺科技有限公司、北京人大金仓信息技术股份有限公司、景腾多媒体股份有限公司、杭州巨峰科技有限公司、乐至（上海）科技有限公司、杭州追速科技有限公司、南通点酷网络科技有限公司、深圳市圆梦云科技有限公司、友讯电子设备（上海）有限公司、上海装盟信息科技有限公司、江阴互盛网络科技有限公司、青岛东胜伟业软件有限公司、上海智休信息科技有限公司、诸城市三剑网络传媒有限公司、北京安天网络安全技术有限公司、中版行知（广州）数字传媒有限公司、南京云创大数据科技股份有限公司、内蒙古万户信息科技有限公司、北京博乐虎科技有限公司、上海亿速网络有限公司、上海物创信息科技有限公司、济南宇霞信息技术有限公司、河南斧牛网络科技有限公司、江苏灵匠信息科技有限公司、廊坊市极致网络科技有限公司、西安佰联网络技术有限公司、上海卓岚信息科技有限公司、深圳市皓峰通讯技术有限公司、四川迅睿云软件开发有限公司、上海呈禹信息科技有限公司、西安三才科技实业有限公司、珠海金山办公软件有限公司、太原迅易科技有限公司、北京超图软件股份有限公司、博睿海航（北京）科技有限公司、洛阳云业信息科技有限公司、小米科技有限责任公司、深圳市景阳科技股份有限公司、上海牛之云网络科技有限公司、宏旺投资集团有限公司、上海商派网络科技有限公司、厦门易商网络科技有限公司、天津黑核科技有限公司、江西铭软科技有限公司、罗克韦尔自动化（中国）有限公司、金华市博创网络科技有限公司、沈阳优诺科技有限公司、天闻数媒科技（北京）有限公司、北京百容千域软件技术开发有限责任公司、北京四月星空网络技术有限公司、逍遥 B2C 商城系统、瑞捷云、保定互动营销、杰科网络设计工作室、月光創意、中国知网、WF 网络团队、极致 CMS、苹果 CMS、推券客联盟、狂雨小说 cms、UCMS、ZZCMS、KKCMS、OFCMS、WMCMS、ShuipFCMS、PTCMS、Catfish CMS、SemCms、BEESCMS、Heybbs、XYCMS、emlog、mblog 、Mantis 和 SEACMS。

本周，CNVD 发布了《Microsoft 发布 2020 年 9 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5719

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、北京神州绿盟科技有限公司、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、山东华鲁科技发展股份有限公司、北京华云安信息技术有限公司河南灵创电子科技有限公司、浙江安腾信息技术有限公司、河南信安世纪科技有限公司、南京众智维信息科技有限公司、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、北京云科安信科技有限公司（Seraph 安全实验室）、长春嘉诚信息技术股份有限公司、吉林谛听信息技术有限公司、北京天地和兴科技有限公司、京东云安全、北京长亭科技有限公司、中科华威（北京）信息技术研究院、北京安华金和科技有限公司、广西等保安全测评有限公司、北京卓识网安技术股份有限公司、北京禹宏信安科技有限公司、华信咨询设计研究院有限公司、杭州安信检测技术有限公司、北京智游网安科技有限公司、平安银河实验室、上海观安信息技术股份有限公司、山东云天安全大数据技术有限公司、四川哨兵信息科技有限公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 4632 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）和上海交大向 CNVD 共享的白帽子报送的 3582 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）	2224	2224
阿里云计算有限公司	946	0
斗象科技（漏洞盒子）	816	816
上海交大	542	542
北京神州绿盟科技有限公司	237	4
哈尔滨安天科技集团股份有限公司	208	0
华为技术有限公司	206	0

北京天融信网络安全技术有限公司	144	4
深信服科技股份有限公司	130	0
中国电信集团系统集成有限责任公司	108	108
新华三技术有限公司	62	0
北京安信天行科技有限公司	8	8
北京启明星辰信息安全技术有限公司	6	6
北京知道创宇信息技术股份有限公司	1	0
国瑞数码零点实验室	199	199
山东华鲁科技发展股份有限公司	71	71
北京华云安信息技术有限公司	31	31
河南灵创电子科技有限公司	29	29
浙江安腾信息技术有限公司	24	24
西门子（中国）有限公司	19	0
河南信安世纪科技有限公司	14	14
杭州迪普科技股份有限公司	13	0
南京众智维信息科技有限公司	12	12
山东云天安全技术有限公司	11	11
远江盛邦（北京）网络安全科技股份有限公司	10	10
北京云科安信科技有限公司（Seraph 安全实验室）	9	9
长春嘉诚信息技术股份有限公司	9	9
吉林谛听信息技术有限公司	9	9
北京天地和兴科技有限公司	8	8

京东云安全	8	8
北京长亭科技有限公司	6	6
中科华威（北京）信息技术研究院	6	6
北京安华金和科技有限公司	4	4
广西等保安全测评有限公司	3	3
北京卓识网安技术股份有限公司	3	3
北京禹宏信安科技有限公司	2	2
华信咨询设计研究院有限公司	2	2
杭州安信检测技术有限公司	1	1
北京智游网安科技有限公司	1	1
平安银河实验室	1	1
上海观安信息技术股份有限公司	1	1
山东云天安全大数据技术有限公司	1	1
四川哨兵信息科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 西藏分中心	1	1
个人	442	442
报送总计	6590	4632

本周漏洞按类型和厂商统计

本周，CNVD 收录了 395 个漏洞。应用程序 202 个，WEB 应用 154 个，操作系统 17 个，智能设备（物联网终端设备）14 个，网络设备（交换机、路由器等网络端设备）6 个，安全产品 2 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	202
WEB 应用	154
操作系统	17
智能设备（物联网终端设备）	14
网络设备（交换机、路由器等网络端设备）	6
安全产品	2

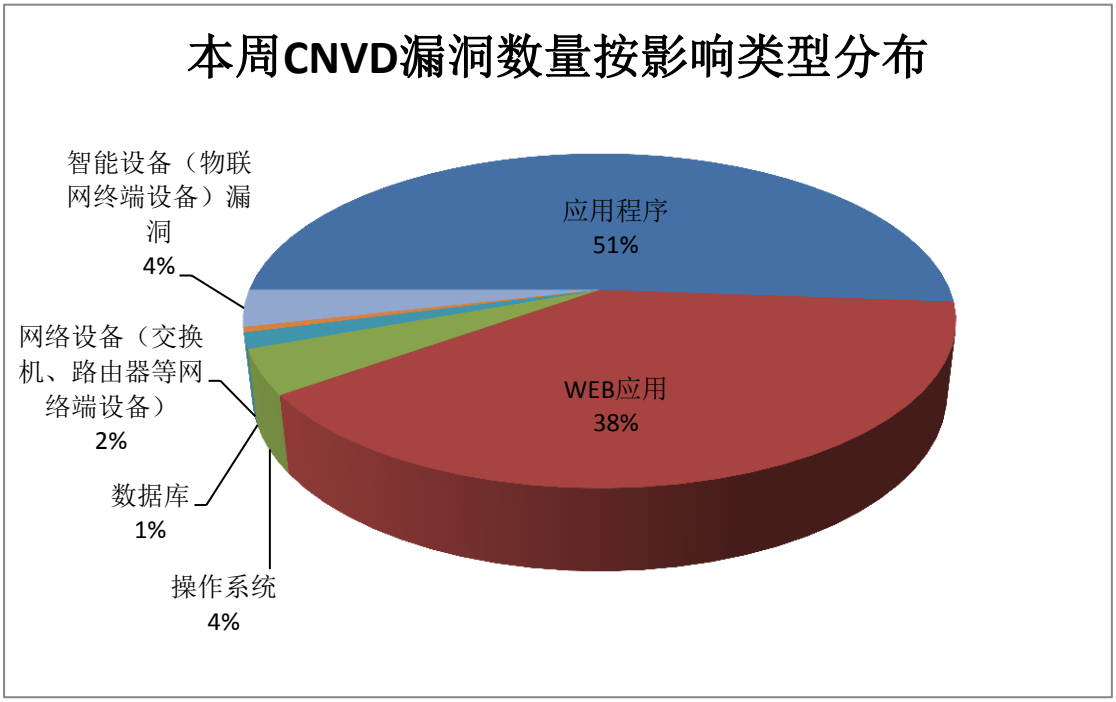

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Siemens、Oracle 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	Cisco	19	5%
2	Siemens	18	4%
3	Oracle	16	4%
4	Apple	15	4%
5	IBM	14	4%
6	CloudBees	12	3%
7	Open Solutions for Education	10	3%
8	Microsoft	9	2%

9	vBulletin	9	2%
10	其他	273	69%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，18 个移动互联网行业漏洞，20 个工控行业漏洞（如下图所示）。其中，“多款 Apple 产品 Audio 组件越界写入漏洞、Siemens Polarion Subversion Webclient 跨站请求伪造漏洞、Cisco FXOS 和 NX-OS 拒绝服务漏洞（CNVD-2020-50560）、DrayTek Vigor3900、Vigor2960 和 Vigor300B 操作系统命令注入漏洞（CNVD-2020-51416）”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/

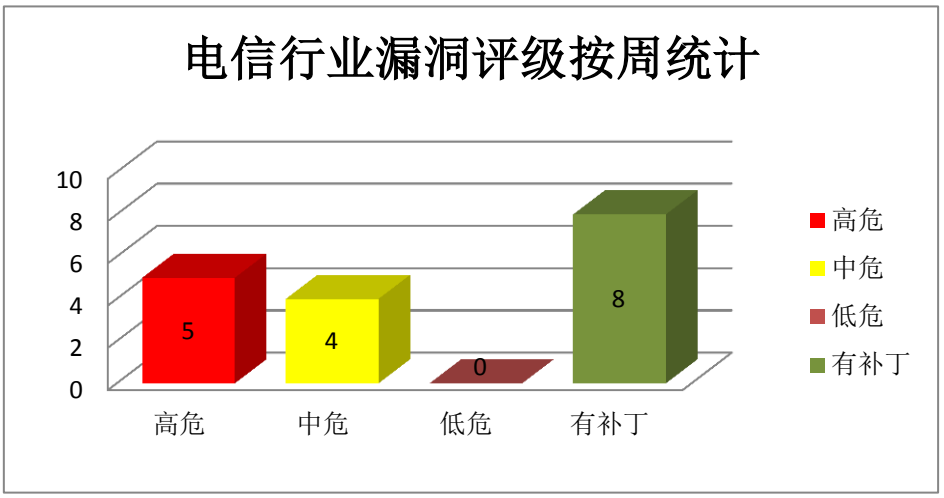

图 3 电信行业漏洞统计

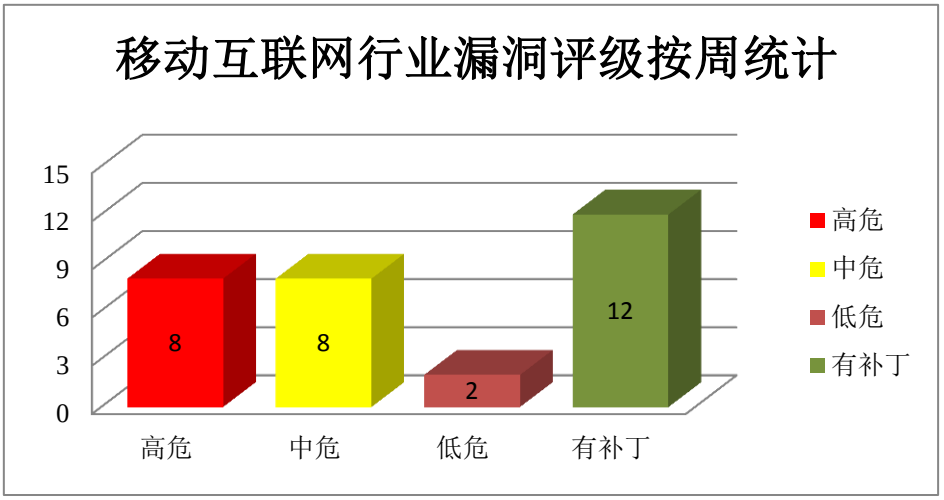

图 4 移动互联网行业漏洞统计

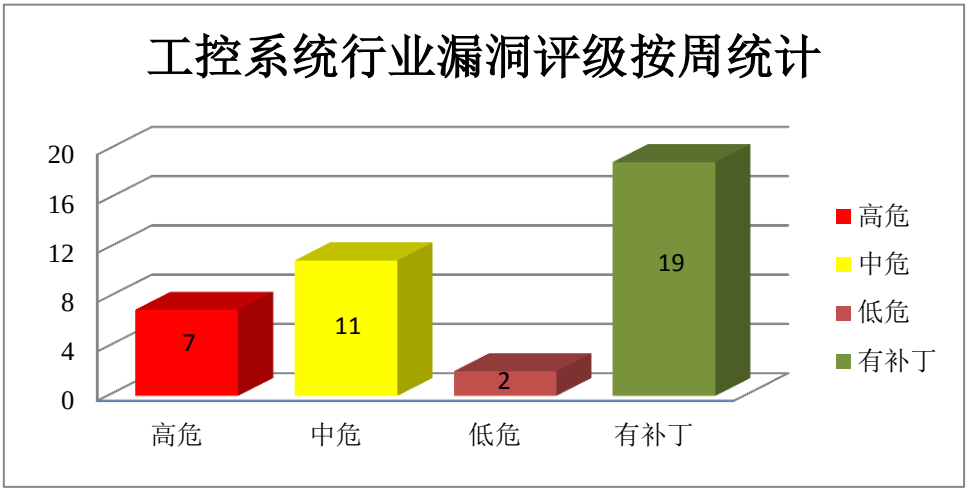

图 5 工控系统行业漏洞统计

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 Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer VBScript Engine 远程代码执行漏洞（CNVD-2020-51780、CNVD-2020-51784、CNVD-2020-51783）、Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2020-51778、CNVD-2020-51782、CNVD-2020-51781）、Microsoft Internet Explorer MSHTML Engine 远程代码执行漏洞、Microsoft Internet Explorer 信息泄露漏洞（CNVD-2020-51786）。其中，除“Microsoft Internet Explorer 信息泄露漏洞（CNVD-2020-51786）”外，其余漏洞的综合评级为“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-2020-51780

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51778

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51784

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51783

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51782

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51781

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51785

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51786

2、Cisco 产品安全漏洞

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 FXOS Software 是一套运行在思科安全设备中的防火墙软件。Cisco SD-WAN Solution 是一套网络扩展解决方案。Cisco AnyConnect Secure Mobility Client for Windows 是一款基于 Windows 平台的可通过任何设备安全访问网络和应用的安全移动客户端。Cisco IOS XR 软件是用于服务提供商网络的模块化和完全分布式的网络操作系统。Cisco Jabber for Windows 是一套用于 Windows 平台的统一通信客户端解决方案。Cisco Webex Training 是一种在线培训解决方案。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管理权限，执行任意代码，导致拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco NX-OS 拒绝服务漏洞（CNVD-2020-50555）、Cisco FXOS 和 NX-OS 拒绝服务漏洞（CNVD-2020-50560）、Cisco SD-WAN Solution 权限许可和访问控制问题漏洞（CNVD-2020-50563）、Cisco AnyConnect Secure Mobility Client for Windows 代码问题漏洞、Cisco IOS XR 权限提升漏洞（CNVD-2020-51772）、Cisco Jabber for Windows 命令注入漏洞、Cisco Webex Training 输入验证错误漏洞、Cisco IOS XR 权限提升漏洞（CNVD-2020-51773）。其中，除“Cisco NX-OS 拒绝服务漏洞（CNVD-2020-50555）、Cisco IOS XR 权限提升漏洞（CNVD-2020-51772）、Cisco Webex Training 输入验证错误漏洞”外，其余漏洞的综合评级为“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-2020-50555
https://www.cnvd.org.cn/flaw/show/CNVD-2020-50560
https://www.cnvd.org.cn/flaw/show/CNVD-2020-50563
https://www.cnvd.org.cn/flaw/show/CNVD-2020-50564
https://www.cnvd.org.cn/flaw/show/CNVD-2020-51772
https://www.cnvd.org.cn/flaw/show/CNVD-2020-51771
https://www.cnvd.org.cn/flaw/show/CNVD-2020-51774
https://www.cnvd.org.cn/flaw/show/CNVD-2020-51773

3、IBM 产品安全漏洞

IBM API Connect 是一种综合的端到端 API 生命周期解决方案。IBM Business Process Manager 是一套综合的业务流程管理平台。IBM Business Automation Workflow 是一套工作流程自动化解决方案。IBM MQ Appliance 是一款用于快速部署企业级消息中间件的一体机设备。IBM InfoSphere Information Server 是一套数据整合平台。IBM Aspera 是一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。IBM Engineering Test Management 是一个协作性的、基于 Web 的质量管理解决方案，可以提供端到端的测试规划和测试资产管理。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安全限制，并将用户重定向到网络钓鱼站点，获取敏感信息，执行任意代码，导致

拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM API Connect 权限提升漏洞（CNVD-2020-50792）、IBM Business Process Manager 和 IBM Business Automation Workflow 安全绕过漏洞、IBM Business Process Manager 和 IBM Business Automation Workflow 信息泄露漏洞、IBM MQ Appliance 拒绝服务漏洞（CNVD-2020-50796）、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-2020-50801）、IBM Aspera Connect 代码执行漏洞、IBM Engineering Test Management 信息泄露漏洞、IBM Engineering Test Management 跨站脚本漏洞。其中，“IBM Aspera Connect 代码执行漏洞”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-2020-50792

https://www.cnvd.org.cn/flaw/show/CNVD-2020-50795

https://www.cnvd.org.cn/flaw/show/CNVD-2020-50794

https://www.cnvd.org.cn/flaw/show/CNVD-2020-50796

https://www.cnvd.org.cn/flaw/show/CNVD-2020-50801

https://www.cnvd.org.cn/flaw/show/CNVD-2020-50800

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51788

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51787

4、Apple 产品安全漏洞

Apple iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Apple iTunes for Windows ImageIO 越界写入漏洞（CNVD-2020-51491、CNVD-2020-51492）、Apple iTunes for Windows ImageIO 组件越界读取漏洞、Apple iTunes for Windows ImageIO 组件远程代码执行漏洞、多款 Apple 产品 GeoServices 组件授权问题漏洞、多款 Apple 产品 Wi-Fi 组件越界读取漏洞、多款 Apple 产品 Audio 组件越界写入漏洞、多款 Apple 产品 WebKit 组件越界读取漏洞（CNVD-2020-51502）。其中，除“多款 Apple 产品 GeoServices 组件授权问题漏洞”外，其余漏洞的综合评级为“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-2020-51491

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51490

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51489

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51492

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51495

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51494

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51499

https://www.cnvd.org.cn/flaw/show/CNVD-2020-51502

5、Mozilla Firefox 资源管理错误漏洞（CNVD-2020-51034）

Mozilla Firefox 是美国 Mozilla 基金会的产品。Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。本周，Mozilla Firefox 产品被披露存在资源管理错误漏洞。攻击者可借助特制的请求利用该漏洞造成拒绝服务。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-2020-51034

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-2020-51036	GnuTLS 拒绝服务漏洞（CNVD-2020-51036）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.gnutls.org/security-new.html#GNUTLS-SA-2020-09-04
CNVD-2020-51035	Linux kernel 代码注入漏洞（CNVD-2020-51035）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security-tracker.debian.org/tracker/CVE-2020-14386
CNVD-2020-51246	Siemens Polarion Subversion Webclient 跨站请求伪造漏洞	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://cert-portal.siemens.com/productcert/pdf/ssa-436520.pdf
CNVD-2020-51517	Veeam ONE 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.veeam.com/kb3221
CNVD-2020-51529	SolarWinds Serv-U FTP Server 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://documentation.solarwinds.com/en/success_center/servu/Content/Release_Notes/Servu_15-2-1_release_notes.htm
CNVD-2020-51538	GitLab 权限提升漏洞（CNVD-2020-51538）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.auscert.org.au/bulletins/ES

			B-2020.3028/
CNVD-2020-51542	Linux kernel 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security-tracker.debian.org/tracker/CVE-2020-14314
CNVD-2020-51557	HCL Technologies Digital Experience 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://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0079840&sys_kb_id=d08aa3e5db15989455f38d6d13961982
CNVD-2020-51555	F5 NGINX Controller 跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K43520321
CNVD-2020-51235	Siemens License Management Utility (LMU)权限提升漏洞	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://cert-portal.siemens.com/productcert/pdf/ssa-709003.pdf

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敏感信息，执行任意代码，破坏内存。此外，Cisco、IBM、Apple 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，并将用户重定向到网络钓鱼站点，获取敏感信息，执行任意代码，导致拒绝服务攻击等。另外，Mozilla Firefox 被披露存在资源管理错误漏洞。攻击者可借助特制的请求利用该漏洞造成拒绝服务。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、Joomla! J2 Store SQL 注入漏洞

验证描述

Joomla!是一套使用 PHP 和 MySQL 开发的开源、跨平台的内容管理系统(CMS)。

Joomla! J2 Store 存在 SQL 注入漏洞。攻击者可利用漏洞执行恶意的 SQL 命令。

验证信息

POC 链接：https://packetstormsecurity.com/files/157999/Joomla-J2-Store-3.3.11-SQL-Injection.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-51485

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. WhatsApp 披露六个以前未公开的漏洞

WhatsApp 修复了其应用程序中六个以前未公开的漏洞，并在一个新的专用安全咨询网站上披露了这些漏洞。其中一些漏洞是通过 Facebook Bug-Bounty 计划报告的，而其他漏洞则是在代码审查期间发现的。

参考链接：https://securityaffairs.co/wordpress/107950/security/whatsapp-undisclosed-flaws.html

2. Adobe 修复了 Adobe InDesign、Framemaker 和 Experience Manager 中的严重漏洞

Adobe 已发布安全更新，修复 12 个关键漏洞，攻击者可以利用这些漏洞在运行 Adobe InDesign、Adobe Framemaker 和 Adobe Experience Manager 易受攻击版本的系统上执行任意代码。

参考链接：https://securityaffairs.co/wordpress/108051/security/adobe-indesign-framemaker-experience-manager-flaws.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