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 28 日-2020 年 10 月 11 日　　2020 年第 40、41 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 169 个，其中高危漏洞 44 个、中危漏洞 111 个、低危漏洞 14 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 42 个（占 25%），其中互联网上出现“iCMS 跨站请求伪造漏洞（CNVD-2020-54957）、WordPress 跨站脚本漏洞（CNVD-2020-54948）”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 3670 个，与上周（2902 个）环比增加 26%。

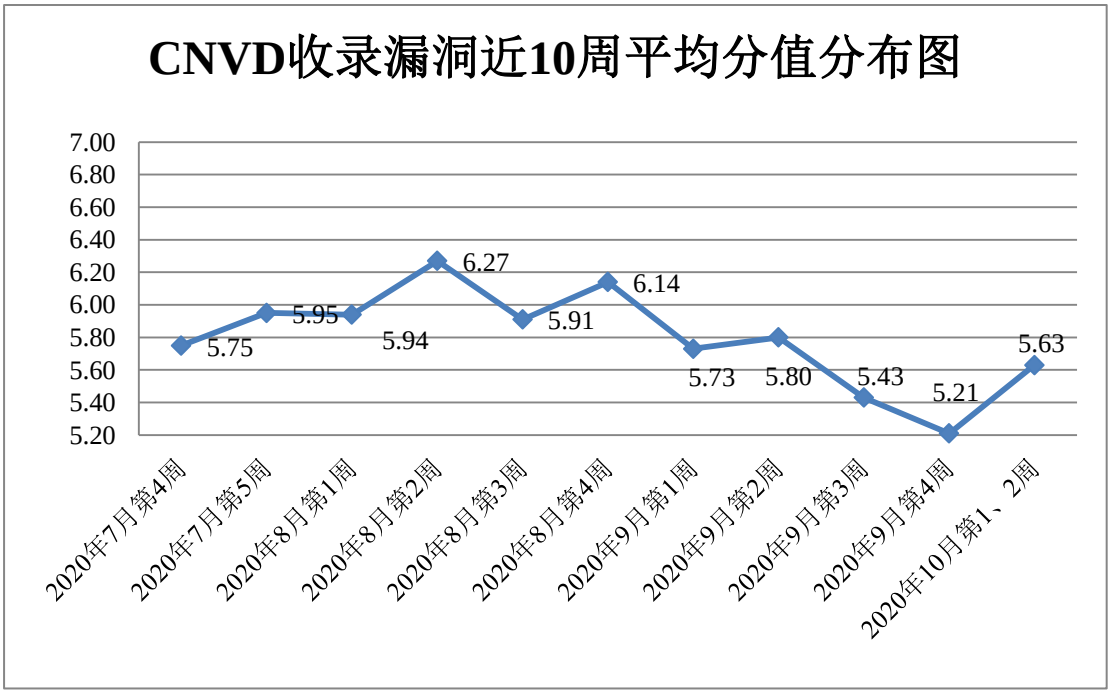

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 起，向基础电

信企业通报漏洞事件 7 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 239 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 41 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 47 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：

西门子（中国）有限公司、深圳市迅雷网络技术有限公司、珠海金山办公软件有限公司、北京四方继保自动化股份有限公司、厦门市灵鹿谷科技有限公司、北京东云创达科技有限公司、上海丹帆网络科技有限公司、天津南大通用数据技术股份有限公司、清宁智能科技石家庄有限公司、福州网钛软件科技有限公司、用友网络科技股份有限公司、北京通达信科科技有限公司、施耐德（Schneider Electric）、剑鱼论坛、TP-LINK、WiseCleaner、Rockwellautomation、IObit 和 Matroska、研华科技（中国）有限公司、湖南壹拾捌号网络技术有限公司、舟山市智慧城市运营有限公司、哈尔滨伟成科技有限公司、淄博闪灵网络科技有限公司、广东凯格科技有限公司、郑州微口网络科技有限公司、四川思途智旅软件有限公司、广东准度科技有限公司、北京华宇信息技术有限公司、南京南瑞集团公司水利水电技术分公司、广州市颖峰信息科技有限公司、通用电气（GE）公司、北京世纪超星信息技术发展有限责任公司、广州红帆科技有限公司、广联达科技股份有限公司、武汉航达航空科技发展有限公司、西安九佳易信息资讯有限公司、郑州卡卡罗特软件科技有限公司、厦门灵鹿谷科技、华科网络、里程密 PHP 博客系统、华夏 ERP、海洋 CMS、PCFCMS、Guojiz、INFRAWARE、MonkeyCode 和 ThinkPHP。

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、北京神州绿盟科技有限公司、新华三技术有限公司、华为技术有限公司、哈尔滨安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。浙江安腾信息技术有限公司、国瑞数码零点实验室、远江盛邦（北京）网络安全科技股份有限公司、安徽长泰信息安全服务有限公司、长春嘉诚信息技术股份有限公司、河南灵创电子科技有限公司 、西安交大捷普网络科技有限公司、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、山东云天安全技术有限公司、山东新潮信息技术有限公司、山东华鲁科技发展股份有限公司、北京网御星云信息技术有限公司、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、深圳市魔方安全科技有限公司、北京安全共识科技有限公司、南京众智维信息科技有限公司、北京智游网安科技有限公司、广西等保安全测评有限公司、平安银河实验室、山东道普测评技术有限公司、长扬科技（北京）有限公司、北京威努特技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、博智安全科技股份有限公司、成都安美勤信息技术股份有限公司、广州安亿信软件科技有限公司、奇安

信-工控安全实验室及其他个人白帽子向CNVD提交了3670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、奇安信网神（补天平台）向CNVD共享的白帽子报送的2254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）	1077	1077
上海交大	704	704
北京天融信网络安全技术有限公司	616	1
奇安信网神（补天平台）	473	473
北京神州绿盟科技有限公司	190	5
新华三技术有限公司	152	0
华为技术有限公司	143	0
哈尔滨安天科技集团股份有限公司	82	0
中新网络信息安全股份有限公司	82	82
北京启明星辰信息安全技术有限公司	56	1
深信服科技股份有限公司	40	0
中国电信集团系统集成有限责任公司	30	30
北京知道创宇信息技术股份有限公司	3	3
浙江安腾信息技术有限公司	120	120
国瑞数码零点实验室	113	113
远江盛邦（北京）网络安全科技股份有限公司	61	61
安徽长泰信息安全服务有限公司	58	58
长春嘉诚信息技术股份有限公司	54	54
河南灵创电子科技有限公	40	40

司		
西安交大捷普网络科技有限公司	31	31
河南信安世纪科技有限公司	29	29
杭州迪普科技股份有限公司	14	14
山东云天安全技术有限公司	13	13
山东新潮信息技术有限公司	10	10
山东华鲁科技发展股份有限公司	8	8
北京网御星云信息技术有限公司	7	7
吉林谛听信息技术有限公司	7	7
北京天地和兴科技有限公司	4	4
京东云安全	4	4
深圳市魔方安全科技有限公司	4	4
北京安全共识科技有限公司	3	3
南京众智维信息科技有限公司	3	3
北京智游网安科技有限公司	2	2
广西等保安全测评有限公司	2	2
平安银河实验室	2	2
山东道普测评技术有限公司	2	2
长扬科技（北京）有限公司	1	1
北京威努特技术有限公司	1	1
北京云科安信科技有限公司（Seraph 安全实验室）	1	1
博智安全科技股份有限公司	1	1

成都安美勤信息技术股份有限公司	1	1
广州安亿信软件科技有限公司	1	1
奇安信-工控安全实验室	1	1
CNCERT 青海分中心	18	18
CNCERT 宁夏分中心	11	11
CNCERT 天津分中心	10	10
CNCERT 山西分中心	7	7
CNCERT 贵州分中心	4	4
CNCERT 上海分中心	3	3
CNCERT 湖南分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 海南分中心	2	2
CNCERT 云南分中心	1	1
个人	636	636
报送总计	4942	3670

本周漏洞按类型和厂商统计

本周，CNVD 收录了 169 个漏洞。应用程序 85 个，WEB 应用 60 个，操作系统 21 个，网络设备（交换机、路由器等网络端设备）2 个，安全产品 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	85
WEB 应用	60
操作系统	21
网络设备（交换机、路由器等网络端设备）	2
安全产品	1

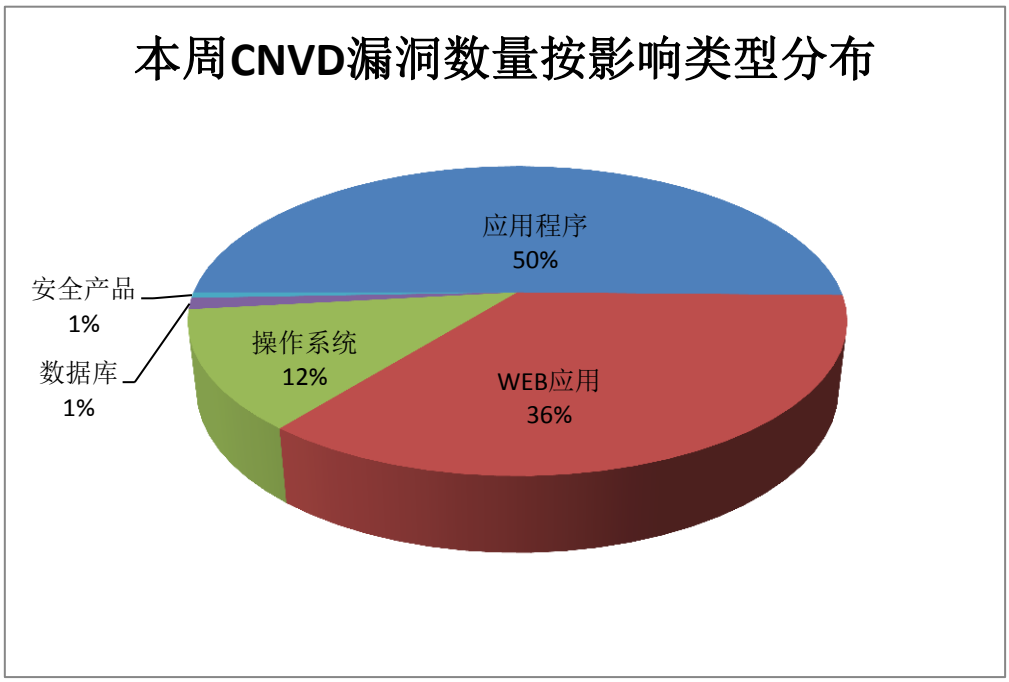

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Artifex Software、Google、IBM 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	Artifex Software	24	14%
2	Google	18	11%
3	IBM	12	7%
4	Mozilla	11	7%
5	cPanel	10	6%
6	Microsoft	10	6%
7	Oracle	10	6%
8	Observium	6	3%
9	珠海金山办公软件有限公司	5	3%
10	其他	63	37%

本周行业漏洞收录情况

本周，CNVD 收录了 2 个电信行业漏洞，12 个移动互联网行业漏洞，其中，“Google Android MediaProvider 权限控制漏洞、Google Android WindowManager 提权漏洞、

Google Android 缓冲区溢出漏洞（CNVD-2020-54471）”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/

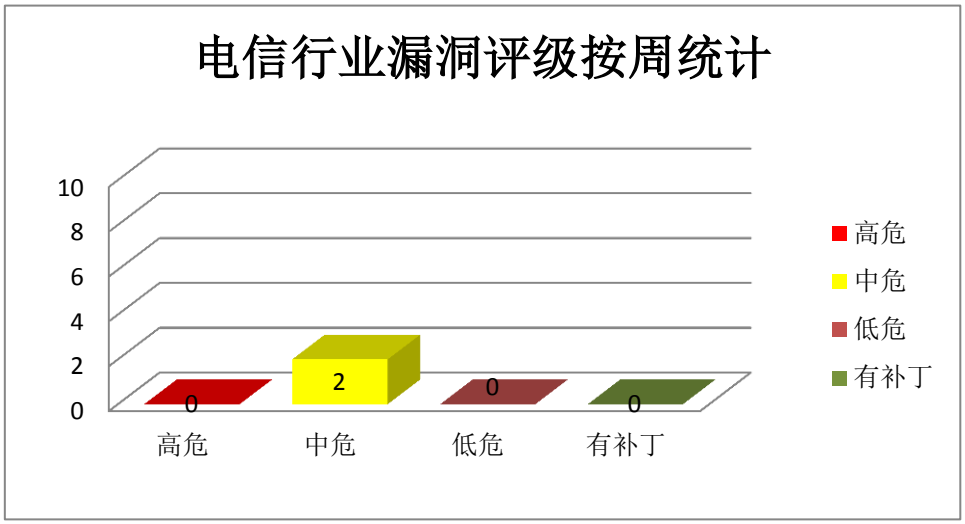

图 3 电信行业漏洞统计

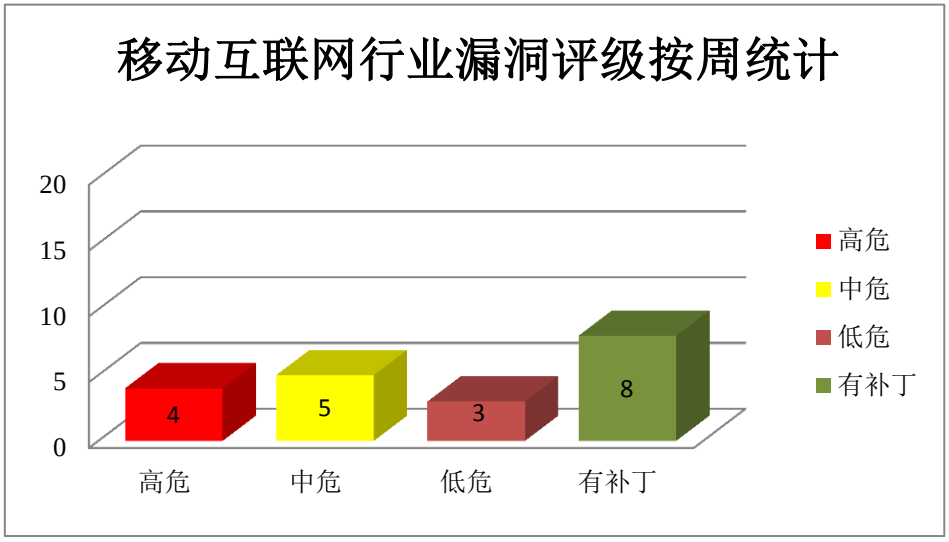

图 4 移动互联网行业漏洞统计

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 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 InstallService 是美国 Microsoft 公司的一个 windows

操作系统的服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以提升的权限执行代码，导致目标系统停止响应。

CNVD 收录的相关漏洞包括：Microsoft Windows 权限提升漏洞（CNVD-2020-54910、CNVD-2020-54907、CNVD-2020-54913）、Microsoft Windows Routing Utilities 拒绝服务漏洞、Microsoft Windows RSoP 权限提升漏洞、Microsoft Windows Language Pack Installer 权限提升漏洞、Microsoft Windows Modules Installer 权限提升漏洞（CNVD-2020-54911）、Microsoft Windows InstallService 权限提升漏洞。其中，“Microsoft Windows 权限提升漏洞（CNVD-2020-54913）、Microsoft Windows Modules Installer 权限提升漏洞（CNVD-2020-54911）、Microsoft Windows 权限提升漏洞（CNVD-2020-54910）”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-2020-54910
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54907
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54913
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54909
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54908
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54912
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54911
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54914

2、IBM 产品安全漏洞

IBM InfoSphere Information Server 是一个数据集成平台。IBM Spectrum Protect（前称 Tivoli Storage Manager）是美国 IBM 公司的一套数据保护平台。IBM DataPower Gateway 是美国 IBM 公司的一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B 和云工作负载而设计的安全和集成平台。IBM Security Secret Server 是美国 IBM 公司的一套特权访问管理解决方案。IBM Business Process Manager 是一套综合的业务流程管理平台。IBM Trusteer Pinpoint 是美国国际商业机器公司（IBM）的一款信息安全保障软件可以检测交易中对方的真实性和交易的风险等级。IBM OpenPages GRC Platform 是美国 IBM 公司的一套用于管理企业风险和合规性的平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞劫持受害者的点击动作，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 点击劫持漏洞、IBM Spectrum Protect 代码执行漏洞（CNVD-2020-54678）、IBM DataPower Gateway 拒绝服务漏洞（CNVD-2020-54934）、IBM Security Secret Server 安全绕过漏洞、IBM Security Secret Server 输入验证错误漏洞、IBM Business Process Manager (Advanced) 和 IBM Business Automation Workflow 信息泄露漏洞、IBM Trusteer Pinpoint 信息泄露

漏洞、IBM OpenPages 跨站脚本漏洞。其中，“IBM Spectrum Protect 代码执行漏洞（CNVD-2020-54678）”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-2020-54317

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54678

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54934

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54933

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54932

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54931

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54938

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54937

3、Google 产品安全漏洞

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。Google TensorFlow 是美国谷歌（Google）公司的一套用于机器学习的端到端开源平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成数据泄露，导致本地特权提升，造成缓存区溢出等。

CNVD 收录的相关漏洞包括：Google Android 缓冲区溢出漏洞（CNVD-2020-54471、CNVD-2020-54466）、Google TensorFlow 输入验证错误漏洞（CNVD-2020-54472、CNVD-2020-54474）、Google Android MediaProvider 权限控制漏洞、Google Android WindowManager 提权漏洞、Google TensorFlow 缓冲区溢出漏洞（CNVD-2020-54782）、Google TensorFlow 代码问题漏洞（CNVD-2020-54781）。其中，“Google Android 缓冲区溢出漏洞（CNVD-2020-54471）、Google TensorFlow 输入验证错误漏洞（CNVD-2020-54472、CNVD-2020-54474）、Google Android MediaProvider 权限控制漏洞、Google Android WindowManager 提权漏洞、Google TensorFlow 缓冲区溢出漏洞（CNVD-2020-54782）、Google TensorFlow 代码问题漏洞（CNVD-2020-54781）”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-2020-54471

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54474

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54472

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54674

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54675

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54782

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54781

https://www.cnvd.org.cn/flaw/show/CNVD-2020-54466

4、Artifex Software 产品安全漏洞

Artifex Ghostscript 是美国 Artifex Software 公司的一款开源的 PostScript（一种用于电子产业和桌面出版领域的页面描述语言和编程语言）解析器。Artifex Software MuPDF 是美国 Artifex Software 公司的一款免费的、轻量级的 PDF 阅读器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致缓冲区溢出或堆溢出，造成解释器崩溃，执行代码等。

CNVD 收录的相关漏洞包括：Artifex Ghostscript 代码执行漏洞、Artifex Software MuPDF 代码问题漏洞、Artifex Ghostscript 拒绝服务漏洞（CNVD-2020-54478、CNVD-2020-54476、CNVD-2020-54475）、Artifex Ghostscript 类型混淆漏洞（CNVD-2020-54479）、Artifex Software MuPDF 缓冲区溢出漏洞（CNVD-2020-54480）、Artifex MuPDF 无限循环漏洞。其中“Artifex Ghostscript 代码执行漏洞、Artifex Software MuPDF 代码问题漏洞”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-2020-54477
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54482
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54476
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54475
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54479
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54478
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54480
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54486

5、Artifex MuPDF 缓冲区溢出漏洞

Artifex MuPDF 是美国 Artifex Software 公司的一款免费的、轻量级的 PDF 阅读器。本周，Artifex MuPDF 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞对可用性造成影响。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-2020-54488

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-2020-54918	GetSimple CMS 跨站脚本漏洞（CNVD-2020-54918）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://get-simple.info/extend/plugin/multi-user/133/
CNVD-2020-	Zoho ManageEngine Applica	高	目前厂商已发布升级补丁以修复漏

54780	tions Manager SQL 注入漏洞（CNVD-2020-54780）		洞，补丁获取链接：https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2020-15394.html
CNVD-2020-54783	Tensorflow 数据验证漏洞	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/tensorflow/tensorflow/releases/tag/v2.3.1
CNVD-2020-54316	PrestaShop 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/PrestaShop/PrestaShop/releases/tag/1.7.6.8
CNVD-2020-54789	Observium SQL 注入漏洞（CNVD-2020-54789）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.observium.org/
CNVD-2020-54467	Facebook HHVM 数据伪造问题漏洞	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.facebook.com/security/advisories/cve-2016-1000004
CNVD-2020-54923	多款 Mozilla 产品缓冲区溢出漏洞（CNVD-2020-54923）	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/mfsa2020-26/
CNVD-2020-54928	Mozilla Thunderbird、Firefox ESR 和 Firefox 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.mozilla.org/en-US/security/advisories/mfsa2020-16/
CNVD-2020-54952	Sequelize SQL 注入漏洞（CNVD-2020-54952）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/sequelize/sequelize/commit/9bd0bc111b6f502223edf7e902680f7cc2ed541e
CNVD-2020-54919	cPanel 代码问题漏洞（CNVD-2020-54919）	高	厂商已发布漏洞修复程序，请及时关注更新：https://docs.cpanel.net/changelogs/88-change-log/

小结：本周，Microsoft、IBM、Google、Artifex Software 等多款产品被披露存在多个漏洞，攻击者可利用漏洞导致本地特权提升，造成缓存区溢出，执行代码，发起拒绝服务攻击等。另外，Artifex MuPDF 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞对可用性造成影响。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、iCMS 跨站请求伪造漏洞（CNVD-2020-54957）

验证描述

iCMS 是一套采用 PHP 和 MySQL 数据库构建的内容管理系统（CMS）。

iCMS v7.0.0 中存在跨站请求伪造漏洞。该漏洞源于 WEB 应用未充分验证请求是否来自可信用户。攻击者可利用该漏洞通过受影响客户端向服务器发送非预期的请求。

验证信息

POC 链接：https://github.com/idreamsoft/iCMS/issues/76

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-54957

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. Microsoft Azure 中存在两个漏洞

微软基于云的 Azure 应用服务中的两个缺陷可能导致服务器端伪造请求（SSFR）和远程代码执行攻击，如果利用这些漏洞，攻击者可以接管管理服务器。

参考链接：https://threatpost.com/microsoft-azure-flaws-servers-takeover/159965/

2. 一组黑客发现 55 个苹果产品相关漏洞 获赏金超 5 万美元

Sam Curry、Brett Buerhaus、Ben Sadeghipour、Samuel Erb 和 Tanner Barnes 花了 3 个月的时间对苹果平台和服务进行黑客攻击，发现了一系列弱点。该团队发现的 55 个漏洞严重程度不一，其中一些漏洞非常严重。由此，获得了超过 5 万美元的除虫奖励。

参考链接：https://www.cnbeta.com/articles/tech/1038075.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