国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 01 月 06 日-2020 年 01 月 12 日　　2020 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 295 个，其中高危漏洞 133 个、中危漏洞 151 个、低危漏洞 11 个。漏洞平均分值为 6.29。本周收录的漏洞中，涉及 0day 漏洞 190 个（占 64%），其中互联网上出现“Mozilla Firefox 拒绝服务漏洞（CNVD-2020-01142）、Microsoft Exchange Server DNS 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 1994 个，与上周（8982 个）环比减少 77%。

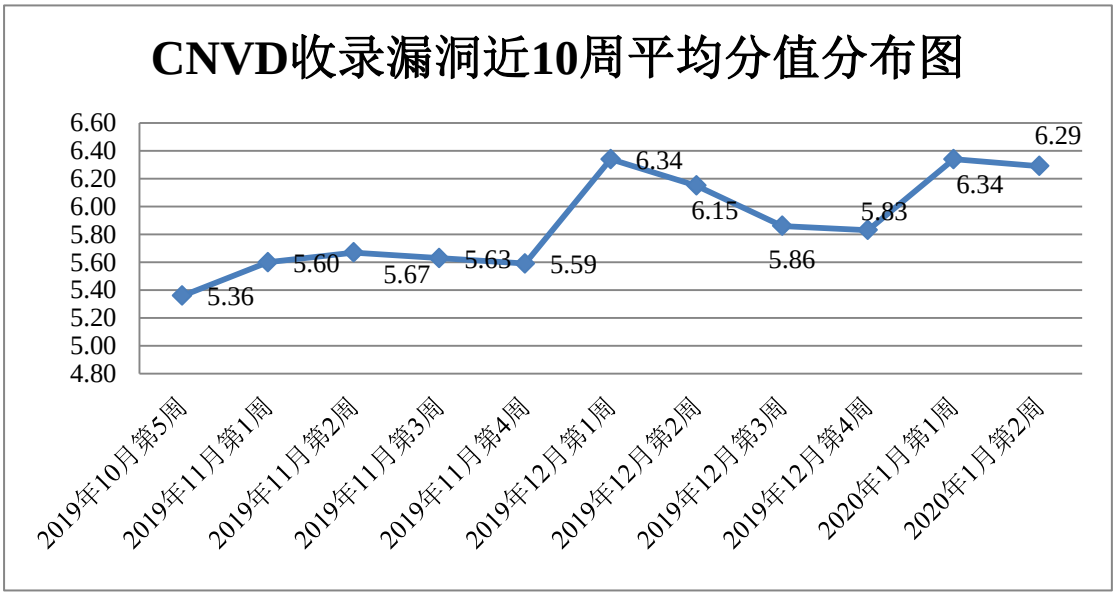

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 起，向基础电信企业通报漏洞事件 10 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 206 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 44 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 12 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：

洛阳云业信息科技有限公司、湖南壹拾捌号网络技术有限公司、北京杰控科技有限公司、湖南中虎网络科技有限公司、西安佰联网络技术有限公司、四平市九州易通科技有限公司、济南点创网络科技有限公司、上海力软信息技术有限公司、石家庄和嘉科技有限公司、中国人民保险集团股份有限公司、义乌畅流网络科技有限公司、Angel 工作室网络网络科技有限公司、深圳市微客互动有限公司、杭州滨兴科技股份有限公司、济南爱程网络科技有限公司、海南易而优科技有限公司、成都康菲顿特网络科技有限公司、六安市开发区鹏程网络工作室、北京天地华大网络技术有限公司、广州合优网络科技有限公司、上海朗铭数码科技有限公司、广州佳朋软件科技有限公司、深圳市安居宝电子有限公司、瑞昱半导体股份有限公司、郑州微口网络科技有限公司、深圳市锟锆科技有限公司、四川迅睿云软件开发有限公司、济宁网络公司、温州优谷科技有限公司、河北鑫考教育科技股份有限公司、北京博乐虎科技有限公司、杭州惊鹊网络科技有限公司、深圳市朗信互联科技有限公司、广州森季软件科技有限公司、中山市华拓信息技术有限公司、湖南潭州教育网络科技有限公司、深圳市蓝色航线科技有限公司、西安众邦网络科技有限公司、广州佳朋软件科技有限公司、酷溜网（北京）科技有限公司、武汉今客软件有限公司、聊城宏远网络科技有限公司、上海泛微网络科技股份有限公司、东方财富信息股份有限公司、昆明云涛科技有限公司、广州天慈网络科技有限公司、浙江宇视科技有限公司、中山市蓝图网络科技有限公司、南通首页信息技术有限公司、国药控股股份有限公司、上海互盾信息科技有限公司、江西金磊科技发展有限公司、上海中科网络信息技术有限公司、北京致远互联软件股份有限公司、欧姆龙自动化（中国）有限公司、沧州市凡诺广告传媒有限公司、上海商创网络科技有限公司、施耐德电气（中国）有限公司、上海荃路软件开发工作室、草根外贸平台、全国信息安全标准化技术委员会秘书处狂雨小说 cms、CBoard 数据可视化平台、YaSM 团队、The Apache Software Foundation、PESCMS、MoMoCMS、yasm、MoMoCMS、DiliCMS 和 phpmywind。

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。河南灵创电子科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、内蒙古洞明科技有限公司、四川月安客信息技术有限

公司、北京冠程科技有限公司、国瑞数码零点实验室、杭州迪普科技股份有限公司、内蒙古奥创科技有限公司、山东云天安全技术有限公司、北京长亭科技有限公司、山东华鲁科技发展股份有限公司、广州三零卫士信息安全有限公司、山东新潮信息技术有限公司、广州美杜莎网络科技有限公司、广州市网迅信息技术有限公司、山石网科通信技术股份有限公司、厦门靠谱云股份有限公司、河南信安世纪科技有限公司、北京智游网安科技有限公司、长春嘉诚信息技术股份有限公司、广州厚极信息科技有限公司及其他个人白帽子向 CNVD 提交了 1994 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 1158 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）	483	483
上海交大	432	432
奇安信网神（补天平台）	243	243
北京天融信网络安全技术有限公司	170	1
哈尔滨安天科技集团股份有限公司	159	0
华为技术有限公司	135	0
深信服科技股份有限公司	127	0
新华三技术有限公司	80	0
恒安嘉新(北京)科技股份公司	74	0
北京神州绿盟科技有限公司	57	6
北京启明星辰信息安全技术有限公司	52	3
厦门服云信息科技有限公司	35	0
四川无声信息技术有限公司	31	31
浙江大华技术股份有限公司	23	23
北京数字观星科技有限公司	20	0

北京知道创宇信息技术股份有限公司	2	0
河南灵创电子科技有限公司	108	108
远江盛邦（北京）网络安全科技股份有限公司	99	99
内蒙古洞明科技有限公司	90	90
四川月安客信息技术有限公司	16	16
北京冠程科技有限公司	16	16
国瑞数码零点实验室	15	15
杭州迪普科技股份有限公司	12	0
内蒙古奥创科技有限公司	9	9
山东云天安全技术有限公司	7	7
北京长亭科技有限公司	5	5
山东华鲁科技发展股份有限公司	5	5
广州三零卫士信息安全有限公司	4	4
山东新潮信息技术有限公司	2	2
广州美杜莎网络科技有限公司	2	2
广州市网迅信息技术有限公司	1	1
山石网科通信技术股份有限公司	1	1
厦门靠谱云股份有限公司	1	1
河南信安世纪科技有限公司	1	1
北京智游网安科技有限公司	1	1
长春嘉诚信息技术股份有限公司	1	1
广州厚极信息科技有限公司	1	1

CNCERT 重庆分中心	20	20
CNCERT 湖南分中心	16	16
CNCERT 四川分中心	4	4
CNCERT 吉林分中心	3	3
CNCERT 贵州分中心	1	1
个人	343	343
报送总计	2907	1994

本周漏洞按类型和厂商统计

本周，CNVD 收录了 295 个漏洞。应用程序 109 个，WEB 应用 91 个，网络设备（交换机、路由器等网络端设备）61 个，操作系统 17 个，安全产品 9 个，智能设备（物联网终端设备）漏洞 7 个，数据库 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	109
WEB 应用	91
网络设备（交换机、路由器等网络端设备）	61
操作系统	17
安全产品	9
智能设备（物联网终端设备）漏洞	7
数据库	1

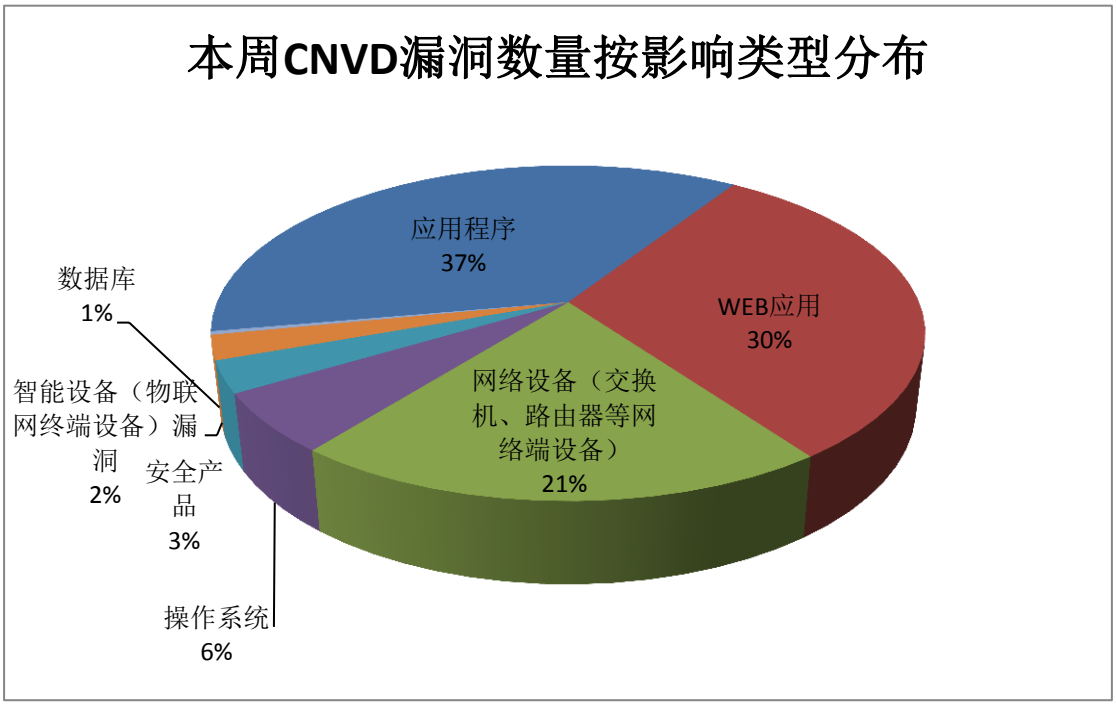

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、Apple、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	Mozilla	11	4%
2	Apple	10	3%
3	Google	10	3%
4	Adobe	9	3%
5	GitLab	9	3%
6	WordPress	9	3%
7	ZTE	8	3%
8	河南拾捌网络技术有限公司	6	2%
9	南京软核科技有限公司	5	2%
10	其他	218	74%

本周行业漏洞收录情况

本周，CNVD 收录了 28 个电信行业漏洞，15 个移动互联网行业漏洞，21 个工控行业漏洞（如下图所示）。其中，“MikroTik's RouterOS 控制台进程内存破坏漏洞、Googl

e Android Framework 权限提升漏洞（CNVD-2020-01294）、多款 Apple 产品 Kernel 组件类型混淆漏洞”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/

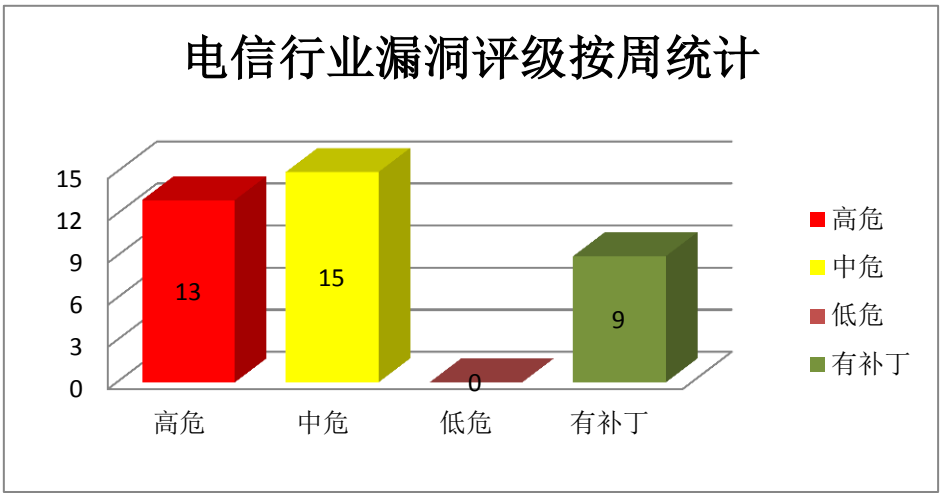

图 3 电信行业漏洞统计

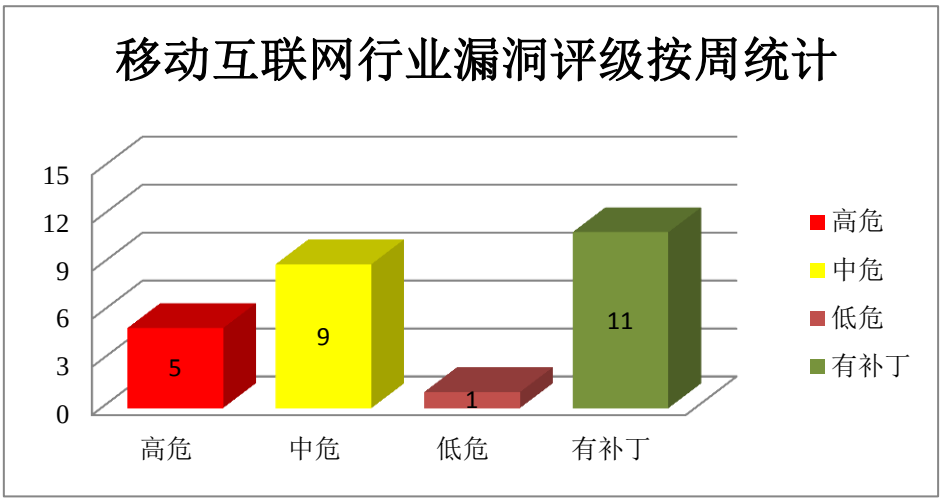

图 4 移动互联网行业漏洞统计

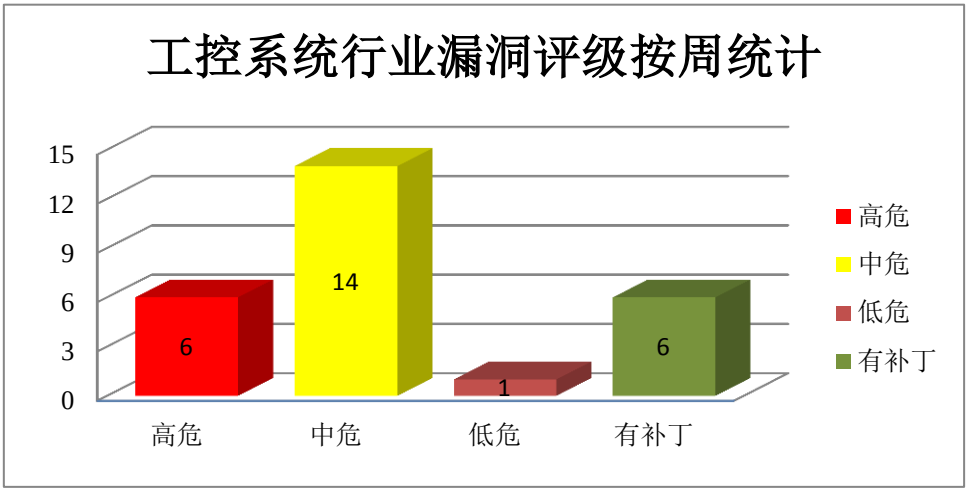

图 5 工控系统行业漏洞统计

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、Mozilla 产品安全漏洞

Mozilla Network Security Services（NSS）是美国 Mozilla 基金会的一个函数库（网络安全服务库）。该产品可跨平台提供 SSL、S/MIME 和其他 Internet 安全标准支持。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，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，获取敏感信息，导致缓冲区溢出等。

CNVD 收录的相关漏洞包括：Mozilla Network Security Services 缓冲区溢出漏洞（CNVD-2020-01173）、Mozilla Firefox 信息泄露漏洞（CNVD-2020-01174）、Mozilla Firefox 和 Mozilla Firefox ESR 跨站脚本漏洞（CNVD-2020-01175）、Mozilla Firefox 和 Mozilla Firefox ESR 代码注入漏洞、Mozilla Firefox 和 Mozilla Firefox ESR 缓冲区溢出漏洞（CNVD-2020-01177）、Mozilla Firefox 和 Firefox ESR 内存错误引用漏洞（CNVD-2020-01179）、Mozilla Firefox 和 Firefox ESR 栈缓冲区溢出漏洞（CNVD-2020-01180）、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2020-01182）。其中，除“Mozilla Firefox 信息泄露漏洞（CNVD-2020-01174）、Mozilla Firefox 和 Mozilla Firefox ESR 跨站脚本漏洞（CNVD-2020-01175）”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-2020-01173

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01174

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01175

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01176

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01177

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01179

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01180

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01182

2、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Swiftshader 是其中的一个开源 3D 渲染工具。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。Framework 是其中的一个 Android 框架组件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，导致拒绝服务，堆损坏。

CNVD 收录的相关漏洞包括：Google Android Framework 拒绝服务漏洞（CNVD-2020-00994）、Google Chrome 资源管理错误漏洞（CNVD-2020-00997、CNVD-2020-00998）、Google Chrome Swiftshader 越界访问漏洞（CNVD-2020-00996、CNVD-2020-01000、CNVD-2020-00999）、Google Android Framework 权限提升漏洞（CNVD-2020-01294、CNVD-2020-01293）。其中，“Google Android Framework 权限提升漏洞（CNVD-2020-01294、CNVD-2020-01293）”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-2020-00994

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00997

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00996

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00998

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00999

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01000

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01294

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01293

3、Apple 产品安全漏洞

Apple iOS 等都是美国苹果（Apple）公司的产品。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 macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple watchOS 是一套智能手表操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，加载未签名的内核扩展，导致缓冲区溢出等。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 组件内存破坏漏洞、Apple macOS Mojave Application Firewall 组件输入验证错误漏洞、多款 Apple 产品 Kernel 组件类型混淆漏洞、多款 Apple 产品 AppleFileConduit 组件内存破坏漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-00537）、Apple macOS Mojave Accessibilit

y Framework 组件缓冲区溢出漏洞、Apple macOS Mojave IOKit 组件验证问题漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2020-00541）。其中，“Apple macOS Mojave Application Firewall 组件输入验证错误漏洞、多款 Apple 产品 Kernel 组件类型混淆漏洞、多款 Apple 产品 AppleFileConduit 组件内存破坏漏洞”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-2020-00532

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00534

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00535

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00531

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00537

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00539

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00540

http://www.cnvd.org.cn/flaw/show/CNVD-2020-00541

4、Adobe 产品安全漏洞

Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Reader 是一套 PDF 文档阅读软件。Adobe Illustrator 是一套基于向量的图像制作软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，获取敏感信息。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2020-01260、CNVD-2020-01261、CNVD-2020-01262、CNVD-2020-01266、CNVD-2020-01265、CNVD-2020-01267）、Adobe Acrobat 和 Reader 权限提升漏洞、Adobe Illustrator 缓冲区溢出漏洞（CNVD-2020-01264）。其中，“Adobe Illustrator 缓冲区溢出漏洞（CNVD-2020-01264）、Adobe Acrobat 和 Reader 权限提升漏洞”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-2020-01260

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01261

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01262

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01264

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01266

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01265

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01267

http://www.cnvd.org.cn/flaw/show/CNVD-2020-01268

5、 WordPress Laborator Neon theme 跨站脚本漏洞

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台，Laborator N

eon theme 是使用在其中的一个网站后台管理主题插件。本周，WordPress Laborator Neon theme 被披露存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。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-2020-00536

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-2020-00517	Huawei M5 lite 10 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://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20191225-01-validation-cn
CNVD-2020-00521	mongo-express 代码执行漏洞	高	厂商已发布相关漏洞补丁链接，请关注厂商主页随时更新：https://github.com/mongo-express
CNVD-2020-01015	munge 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://github.com/dun/munge
CNVD-2020-01016	Strapi Admin 面板 Install and Uninstall Plugin 组件远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/strapi/strapi/pull/4636
CNVD-2020-01014	Envoy 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://istio.io/news/security/istio-security-2019-007/
CNVD-2020-01148	OpenCV 缓冲区溢出漏洞（CNVD-2020-01148）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://opencv.org/
CNVD-2020-01160	Waitress 环境问题漏洞	高	目前厂商已发布相关漏洞补丁修复链接，请及时更新：https://github.com/Pylons/waitress/commit/11d9e138125ad46e951027184b13242a3c1de017
CNVD-2020-01186	Docker 资源管理错误漏洞	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.docker.com/
CNVD-2020-01275	D-Link DAP-1860 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.dlink.com/
CNVD-2020-01315	NeuVector 身份验证漏洞	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://neuvector.com/

小结：本周，Mozilla 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，获取敏感信息，导致缓冲区溢出等。此外，Google、Apple、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致拒绝服务等。另外，WordPress Laborator Neon theme 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。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、Mozilla Firefox 拒绝服务漏洞（CNVD-2020-01142）

验证描述

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。

Mozilla Firefox 存在拒绝服务漏洞。允许攻击者发送特制构建的 URL，使远程用户浏览器崩溃/挂起。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=34686

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-01142

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. Mozilla 释出补丁修复一个正被利用的 Firefox 漏洞

Mozilla 释出了 Firefox v72.0.1 和 ESR 68.4.1，紧急修复了一个正被利用的漏洞。该漏洞属于类型混淆，影响 IonMonkey，它是 Firefox JS 引擎 SpiderMonkey 的 JIT 编译器。该漏洞由中国安全公司奇虎 360 发现和报告，细节没有披露。该公司在一则已删除的推文中称，IE 也有一个 0day 漏洞也正被利用。这是 Mozilla 在过去一年修复的第三个 0day 漏洞。

参考链接：https://www.solidot.org/story?sid=63215

2. TikTok 修复了可能使黑客操纵帐户并访问个人数据的安全漏洞

CheckPoint 的研究人员发现，视频共享和社交网络应用程序 TikTok 中的安全漏洞（已被全球超过 10 亿的 Android 和 iPhone 用户下载）可能会使用户的隐私受到威胁，使攻击者能够操纵用户帐户并暴露个人数据，包括姓名，电子邮件地址和生日。目前不能确认该漏洞是否被利用，但已经修复。

参考链接：https://www.zdnet.com/article/tiktok-fixes-security-flaws-that-could-have-let-hackers-manipulate-accounts-access-personal-data/

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