国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 06 月 22 日-2020 年 06 月 28 日　　2020 年第 26 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 259 个，其中高危漏洞 104 个、中危漏洞 130 个、低危漏洞 25 个。漏洞平均分值为 5.97。本周收录的漏洞中，涉及 0day 漏洞 83 个（占 32%），其中互联网上出现“Savant Web Server 拒绝服务漏洞、vCloud Director 远程代码执行漏洞”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 3522 个，与上周（3718 个）环比减少 5%。

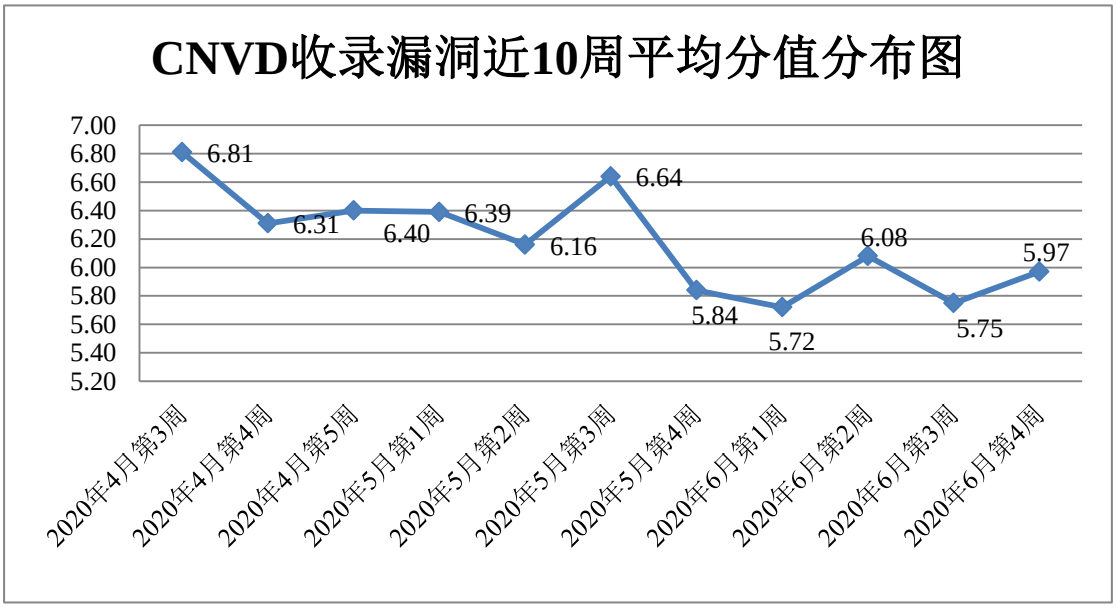

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 326 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 16 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：

深圳市龙脉网络科技有限公司、上海丹帆网络科技有限公司、广州盈可视电子科技有限公司、郑州思创网络技术有限公司、深圳市锟锆科技有限公司、河北世窗信息技术股份有限公司、辽宁微时光科技有限公司、北京海腾时代科技有限公司、珠海金山办公软件有限公司、成都汇高软件有限公司 、杭州凡龙科技有限公司、用友网络科技股份有限公司、北京经纬智慧信息科技有限公司、廊坊市极致网络科技有限公司、北京亚控科技发展有限公司、海南赞赞网络科技有限公司、上海覆盆子信息科技有限公司、上海软众网络科技有限公司、南京广推网络科技有限公司、上海海典软件股份有限公司、深圳市龙艺脉网络科技有限公司、江苏三希科技股份有限公司、上海孚盟软件有限公司、青岛商至信网络科技有限公司、世纪星网络信息服务有限公司、遵义欣腾达信息技术有限公司、研华科技（中国）有限公司、泰安易搜网络有限公司、河南景秀文化传播有限公司、广州双启网络科技有限公司、保定市互动企业营销策划有限公司、南京维拓科技股份有限公司、首岳资讯网路股份有限公司、内蒙古浩海商贸有限公司、杭州巴零科技有限公司、校无忧科技网络公司、四川迅睿云软件开发有限公司、重庆特迪科技有限公司、北京天融信科技有限公司、友讯电子设备（上海）有限公司、四川中疗网络科技有限公司、漳州市芗城科信信息服务有限公司、海南椰角网络科技有限公司、东莞市新势力网络科技有限公司、艾科瑞（北京）仪器仪表有限公司、哈尔滨奇讯科技有限公司、宿迁鑫潮信息技术有限公司、汉中启元动力网络有限公司、沧州市凡诺广告传媒有限公司、北京至诚悠远科技有限公司、上海卓岚信息科技有限公司、福州网钛软件科技有限公司、安徽魅课信息科技有限公司、正方软件股份有限公司、成都生动网络科技有限公司、和利时集团、易迅软件工作室、上海荃路软件开发工作室、兴化市信网信息咨询服务部、信呼 OA 办公系统、Yaazhini、Zzzcms、KUKA、ForU CMS 和 NoneCms。

本周，CNVD 发布了《关于 Apache Spark 存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5585

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、恒安嘉新(北京)科技股份公司、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、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、长春嘉诚信息技术股份有限公司、北京华云安信息技术有

限公司、杭州迪普科技股份有限公司、河南灵创电子科技有限公司 、山东道普测评技术有限公司、上海观安信息技术股份有限公司、山东云天安全技术有限公司、北京顶象技术有限公司、吉林谛听信息技术有限公司、广州安亿信软件科技有限公司、广州竞远安全技术股份有限公司、博智安全科技股份有限公司、北京天地和兴科技有限公司、国家互联网应急中心、内蒙古奥创科技有限公司、北京长亭科技有限公司、京东云安全、北京智游网安科技有限公司、河南信安世纪科技有限公司、国网山东省电力公司、深圳市魔方安全科技有限公司及其他个人白帽子向 CNVD 提交了 3522 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 2579 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）	1565	1565
阿里云计算有限公司	784	0
奇安信网神（补天平台）	554	554
上海交大	460	460
恒安嘉新(北京)科技股份公司	392	0
北京天融信网络安全技术有限公司	340	4
哈尔滨安天科技集团股份有限公司	218	0
北京启明星辰信息安全技术有限公司	150	24
华为技术有限公司	107	0
深信服科技股份有限公司	84	0
中国电信集团系统集成有限责任公司	58	58
新华三技术有限公司	48	0
北京神州绿盟科技有限公司	27	13
西安四叶草信息技术有限公司	25	25
北京奇虎科技有限公司	7	7

北京知道创宇信息技术股份有限公司	5	1
北京数字观星科技有限公司	4	4
远江盛邦（北京）网络安全科技股份有限公司	130	130
长春嘉诚信息技术股份有限公司	95	95
北京华云安信息技术有限公司	42	42
杭州迪普科技股份有限公司	25	0
河南灵创电子科技有限公司	24	24
山东道普测评技术有限公司	17	17
上海观安信息技术股份有限公司	14	14
山东云天安全技术有限公司	13	13
北京顶象技术有限公司	6	6
吉林谛听信息技术有限公司	6	6
广州安亿信软件科技有限公司	4	4
广州竞远安全技术股份有限公司	4	4
博智安全科技股份有限公司	3	3
北京天地和兴科技有限公司	2	2
国家互联网应急中心	2	2
内蒙古奥创科技有限公司	1	1
北京长亭科技有限公司	1	1
京东云安全	1	1
北京智游网安科技有限公司	1	1
河南信安世纪科技有限公司	1	1

国网山东省电力公司	1	1
深圳市魔方安全科技有限公司	1	1
CNCERT 重庆分中心	15	15
CNCERT 西藏分中心	6	6
CNCERT 河北分中心	3	3
CNCERT 宁夏分中心	1	1
CNCERT 广西分中心	1	1
个人	412	412
报送总计	5660	3522

本周漏洞按类型和厂商统计

本周，CNVD 收录了 259 个漏洞。应用程序 130 个，WEB 应用 61 个，操作系统 54 个，网络设备（交换机、路由器等网络端设备）11 个，智能设备（物联网终端设备）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	130
WEB 应用	61
操作系统	54
网络设备（交换机、路由器等网络端设备）	11
智能设备（物联网终端设备）	2
安全产品	1

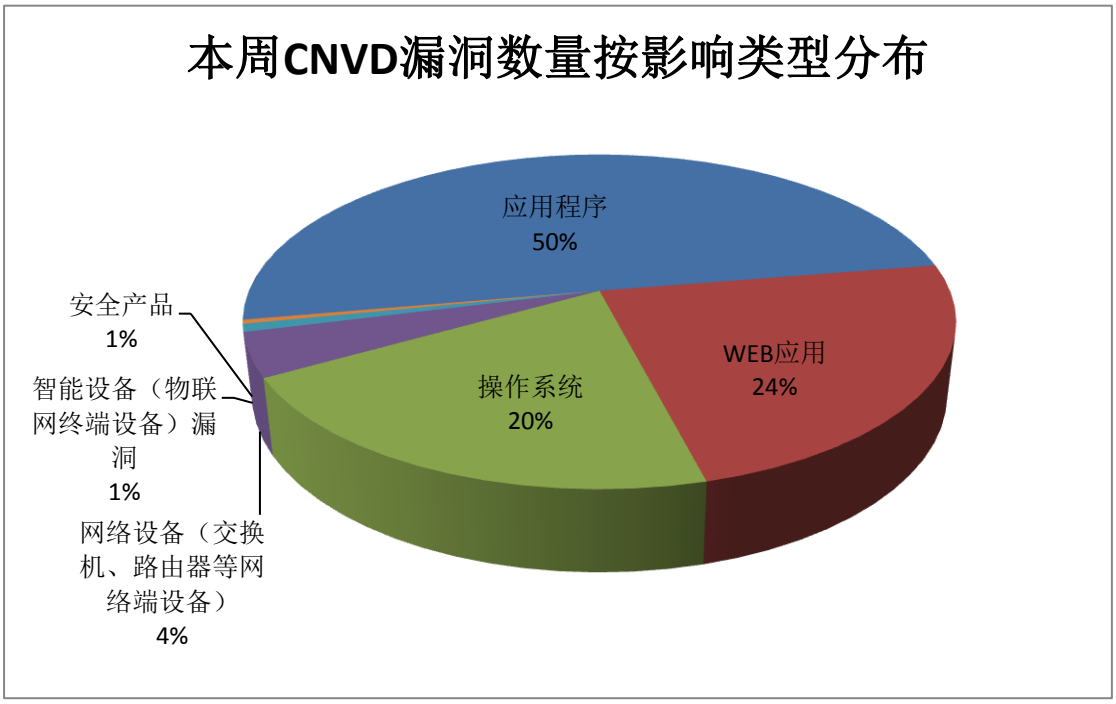

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、珠海金山办公软件有限公司、Apple 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	Google	28	11%
2	珠海金山办公软件有限公司	26	10%
3	Apple	20	8%
4	Cisco	20	8%
5	Treck	19	7%
6	Microsoft	13	5%
7	Adobe	9	3%
8	Intel	8	3%
9	Mitsubishi Electric	5	2%
10	其他	111	43%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，44 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-34328）、

多款 Apple 产品 ImageIO 组件缓冲区溢出漏洞、Samsung 移动设备输入验证错误漏洞（CNVD-2020-34729）、Mitsubishi Electric MC Works64 和 MC Works32 缓冲区溢出漏洞”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/

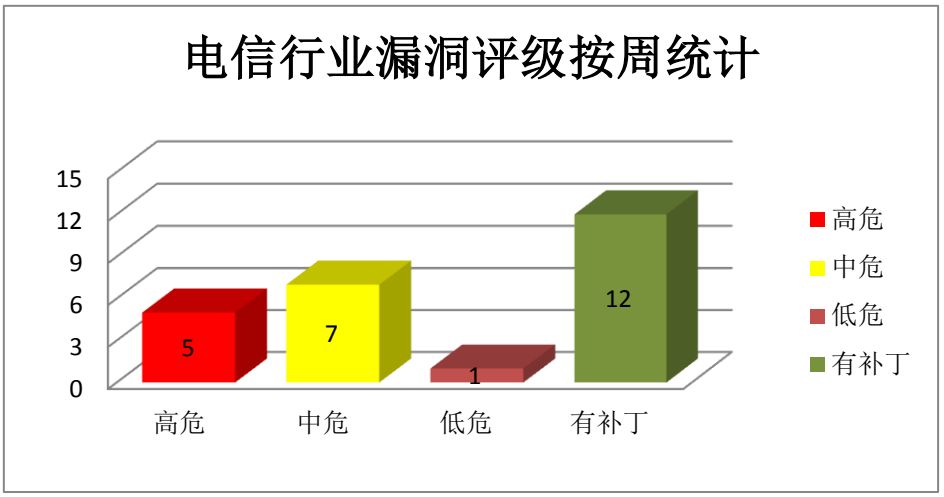

图 3 电信行业漏洞统计

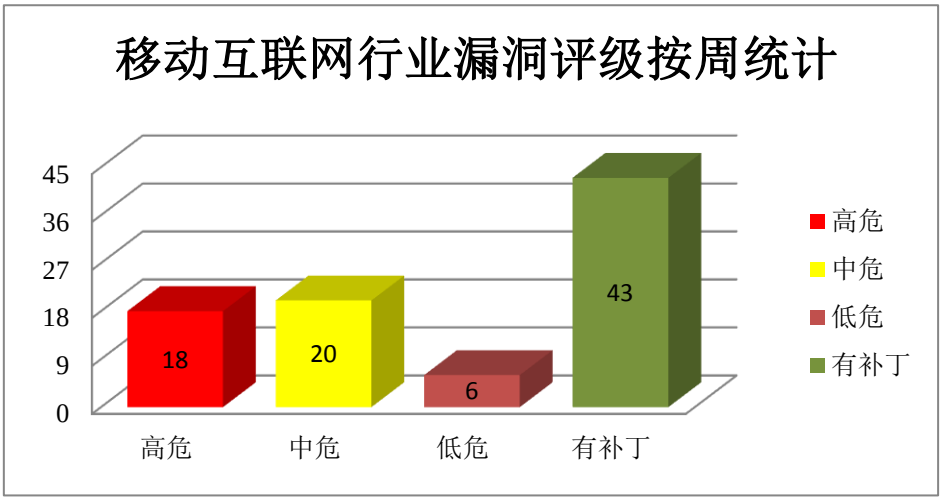

图 4 移动互联网行业漏洞统计

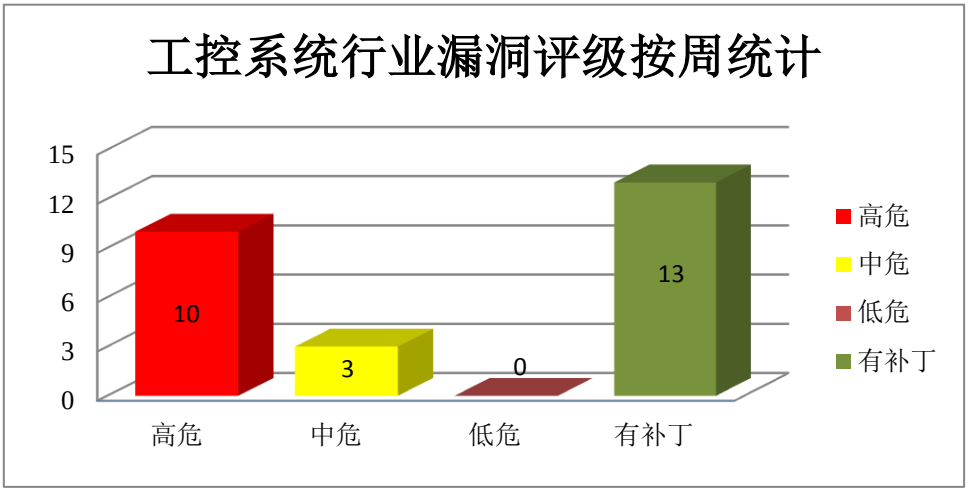

图 5 工控系统行业漏洞统计

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、 Apple 产品安全漏洞

Apple iOS 是一套为移动设备所开发的操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Apple tvOS 是一套智能电视操作系统。Apple macOS Catalina 是一套专为 Mac 计算机所开发的专用操作系统。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内核内存，获取 root 权限，执行任意代码等。

CNVD 收录的相关漏洞包括：多款 Apple 产品 Kernel 组件信息泄露漏洞（CNVD-2020-34135）、Apple macOS Catalina PackageKit 组件权限提升漏洞、多款 Apple 产品 Audio 组件缓冲区溢出漏洞（CNVD-2020-34930、CNVD-2020-34931）、多款 Apple 产品 FontParser 组件缓冲区溢出漏洞、多款 Apple 产品 Kernel 组件缓冲区溢出漏洞（CNVD-2020-34936）、多款 Apple 产品 ImageIO 组件缓冲区溢出漏洞（CNVD-2020-34935、CNVD-2020-34937）。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-2020-34135

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34631

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34930

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34933

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34931

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34936

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34935

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34937

2、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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞覆盖目标文件，提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows Win32k 提权漏洞（CNVD-2020-33800）、Microsoft Windows Storage Service 提权漏洞、Microsoft Windows DirectX 提权漏洞（CNVD-2020-33803）、Microsoft Windows Graphics Device Interface 提权漏洞、Microsoft Windows Graphics Component 提权漏洞（CNVD-2020-33807）、Microsoft Windows Push Notification Service 提权漏洞（CNVD-2020-33805）、Microsoft Windows Error Reporting Manager 提权漏洞、Microsoft Windows Graphics Device Interface 远程代码执行漏洞（CNVD-2020-34941）。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-2020-33800

https://www.cnvd.org.cn/flaw/show/CNVD-2020-33804

https://www.cnvd.org.cn/flaw/show/CNVD-2020-33803

https://www.cnvd.org.cn/flaw/show/CNVD-2020-33801

https://www.cnvd.org.cn/flaw/show/CNVD-2020-33807

https://www.cnvd.org.cn/flaw/show/CNVD-2020-33805

https://www.cnvd.org.cn/flaw/show/CNVD-2020-33808

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34941

3、Cisco 产品安全漏洞

Cisco Webex Meetings Desktop App 是一款使用在桌面环境上的视频会议控制应用程序。Cisco UCS Director 是一套私有云基础架构即服务（IaaS）的异构平台。Cisco Small Business RV320 等是一款 VPN 路由器。Cisco Small Business RV016 Multi-WAN VPN 等是一款 VPN 路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞覆盖文件系统中的任意文件，导致设备崩溃，以 root 用户特权执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Webex Meetings Desktop App 信任管理问题漏洞、Cisco Webex Meetings Desktop App 输入验证错误漏洞、Cisco UCS Director 路径遍历漏洞（CNVD-2020-34295）、多款 Cisco 产品缓冲区溢出漏洞（CNVD-2020-34325、CNVD-2020-34324、CNVD-2020-34328、CNVD-2020-34327、CNVD-2020-34326）。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-2020-34285

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34287

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34295

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34325

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34324

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34328

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34327

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34326

4、Adobe 产品安全漏洞

Adobe Audition 是一个专业音频编辑和混合环境。Adobe Premiere Rush 是 Adobe 推出的一款轻量级视频编辑软件。Adobe Premiere Pro 是一款视频编辑软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Audition 越界写入漏洞（CNVD-2020-34119、CNVD-2020-34120）、Adobe Premiere Rush 越界写入漏洞（CNVD-2020-34122、CNVD-2020-34123）、Adobe Premiere Rush 越界读取漏洞（CNVD-2020-34121）、Adobe Premiere Pro 越界写入漏洞（CNVD-2020-34125、CNVD-2020-34126）、Adobe Premiere Pro 越界读取漏洞（CNVD-2020-34124）。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-2020-34119

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34122

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34121

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34120

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34125

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34124

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34123

https://www.cnvd.org.cn/flaw/show/CNVD-2020-34126

5、Micro Focus ArcSight Enterprise Security Manager 跨站脚本漏洞

Micro Focus ArcSight Enterprise Security Manager 是一套具有事件关联和安全分析功能的企业安全管理软件。本周，Micro Focus ArcSight Enterprise Security Manager 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。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-2020-34716

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	修复方式

		评级	
CNVD-2020-34133	NEC ESMPRO Manager 远程代码执行漏洞	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.necam.com/
CNVD-2020-34255	Treck IPv6 stack 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://treck.com/vulnerability-response-information/
CNVD-2020-34299	Ruby on Rails 跨站请求伪造漏洞（CNVD-2020-34299）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://weblog.rubyonrails.org/2020/5/18/Rails-5-2-4-3-and-6-0-3-1-have-been-released/
CNVD-2020-34302	Red Hat Ceph 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://ceph.io/releases/v15-2-2-octopus-released/
CNVD-2020-34445	Apache Spark 远程代码执行漏洞	高	Apache 官方已发布新版本修复此漏洞，CNVD 建议用户立即升级至最新版本：https://github.com/apache/spark/releases
CNVD-2020-34447	TIBCO Software TIBCO JasperReports Server 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.tibco.com/support/advisories/2020/05/tibco-security-advisory-may-19-2020-tibco-jasperreports-server
CNVD-2020-34646	Johnson Controls Kantech EntraPass 访问控制错误漏洞	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.johnsoncontrols.com/-/media/jci/cyber-solutions/product-security-advisories/2020/jci-psa-2020-6-v1-kantech-entrapass-security-management-software.pdf?la=en&hash=2CC411E20B2BC12B9CE733BA6628740FD925DBA5
CNVD-2020-34653	Mozilla Firefox 和 Firefox ESR 输入验证错误漏洞（CNVD-2020-34653）	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/mfsa2020-16/
CNVD-2020-34706	Intel AMT 和 ISM 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-002

			95.html
CNVD-2020-34720	Meetecho Janus 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://github.com/meetecho/janus-gateway/pull/2214/commits/90cc2ada775c4d4d8f6ae66f96b4ec7588e4bc86

小结：本周，Apple 产品被披露存在多个漏洞，攻击者可利用漏洞读取内核内存，获取 root 权限，执行任意代码等。此外，Microsoft、Cisco、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞覆盖目标文件，提升权限，执行任意代码，导致设备崩溃等。另外，Micro Focus ArcSight Enterprise Security Manager 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、Savant Web Server 拒绝服务漏洞

验证描述

Savant Web Server 是一款 WEB 服务器。

Savant Web Server 存在拒绝服务漏洞。攻击者可利用漏洞发起拒绝服务攻击。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35688

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-34118

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. NVIDIA 解决了 GPU 驱动程序中的多个代码执行问题

NVIDIA 发布了针对 GPU 显示驱动程序和 vGPU 软件中的 12 个漏洞安全补丁，其中一些漏洞可能导致代码执行。影响 GPU 驱动程序的最严重漏洞之一是影响 NVIDIA GPU 显示驱动程序的 CVE-2020-5962，本地攻击者可能利用它来提升特权或导致拒绝服务（DoS）状态。

参考链接：https://securityaffairs.co/wordpress/105273/security/nvidia-code-execution-flaws.html

2. 星巴克新漏洞：可访问 1 亿客户记录

Sam 花了一整天的尝试，仍然没有在 Verizon Media 漏洞赏金计划中有所收获，于是，他决定先退出做一些其他事情。他上网准备订购星巴克的礼品卡，作为朋友的生日礼物。当 sam 在星巴克官网上试图购买时，他发现了 API 调用的可疑之处：在以“ / bff / proxy /”为前缀的 API 下发送了一些请求，但这些请求返回的数据似乎来自另一台主机。

参考链接：https://www.freebuf.com/news/240839.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