国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 07 月 27 日-2020 年 08 月 02 日　　2020 年第 31 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 292 个，其中高危漏洞 82 个、中危漏洞 152 个、低危漏洞 58 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 86 个（占 29%），其中互联网上出现“eGroupWare 'spellchecker.php'远程代码执行漏洞、Frigate Professional 'Pack File'缓冲区溢出漏洞”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 2739 个，与上周（3433 个）环比减少 20%。

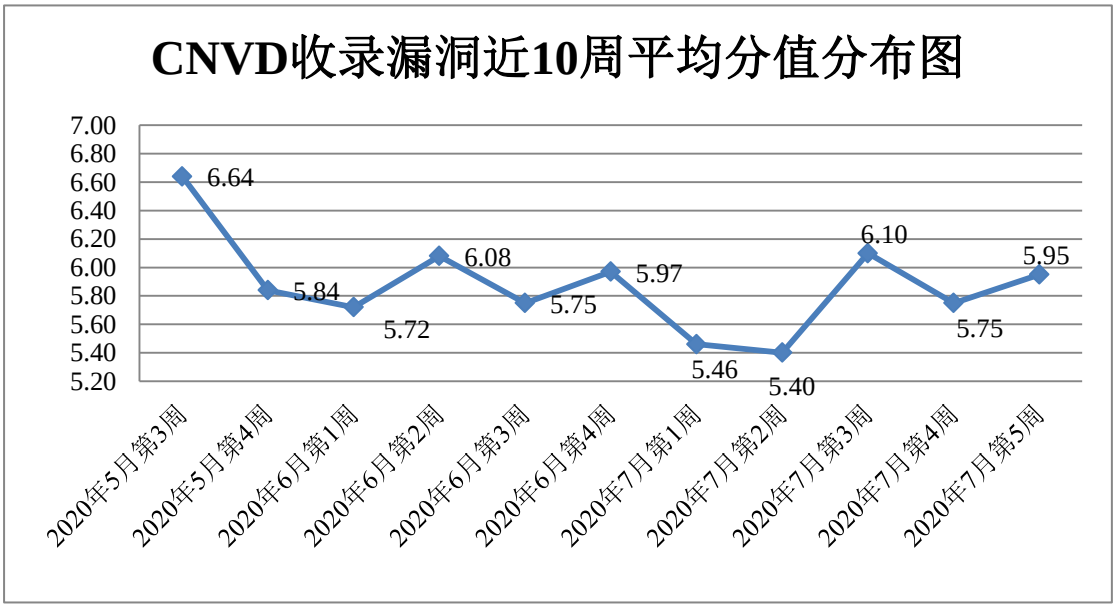

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 起，向基础电信企业通报漏洞事件 5 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 292 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 32 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 33 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：

深圳市网心科技有限公司、常州市青之峰网络科技有限公司、上海丹帆网络科技有限公司、太原迅易科技有限公司、山西尚品优创科技股份有限公司、义乌市创博网络科技有限公司、北京万维盈创科技发展有限公司、北京人大金仓信息技术股份有限公司、南昌市博然科技有限公司、深圳市华磊信息科技有限公司、北京通达信科科技有限公司、诸城市三剑网络传媒有限公司、上海金桥信息股份有限公司、杭州涂鸦科技有限公司、深圳市圆梦云科技有限公司、江苏智汇信息技术有限公司、西安佰联网络技术有限公司、微软（中国）有限公司、山西牛酷信息科技有限公司、南通点酷网络科技有限公司、合肥彼岸互联信息技术有限公司、中国建筑股份有限公司、安徽龙讯信息科技有限公司、上海智休信息科技有限公司、深圳华磊物流通信息科技有限公司、合肥明信软件技术有限公司、三菱电机自动化（中国）有限公司、廊坊市极致网络科技有限公司、深圳迅雷网络技术有限公司、珠海国津软件科技有限公司、甘肃修森网络信息科技有限公司、张家港市易盟电子商务有限公司、杭州吉拉科技有限公司、沈阳盘古网络技术有限公司、北京完美创意科技有限公司、湖南翱云网络科技有限公司、中凯信息网络有限公司、台达电子企业管理(上海)有限公司、深圳市网狐科技有限公司、上海诣策信息科技有限公司、广州搜浪网络科技有限公司、北京米尔伟业科技公司、洛阳市万谦网络科技有限公司、成都康菲顿特网络科技有限公司、南京酷奇信息科技有限公司、哈尔滨巨耀网络科技有限公司、高等教育出版社有限公司、联奕科技有限公司、江苏国泰新点软件有限公司、上海卓卓网络科技有限公司、东方博冠（北京）科技有限公司、镇江明润信息科技有限公司、贵阳同心软件科技有限公司、河南卓奇信息技术有限公司、海南易而优科技有限公司、西安丝路智慧科技有限公司、成都飞鱼星科技股份有限公司、天津南大通用数据技术股份有限公司、深圳市迅雷网络技术有限公司、海南赞赞网络科技有限公司、霍尔果斯鸿鹭华阅文化传播有限公司、深圳市天地心网络技术有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、广州市华企网络科技有限公司、西门子（中国）有限公司、哈工大大数据集团（哈尔滨）农林有限公司、西安华尚软件科技有限公司、喆企网络科技（上海）有限公司、安徽阳光心健科技发展有限公司、西安三才科技实业有限公司、洛阳云业信息科技有限公司、福州亿虎云科技有限公司、珠海金山办公软件有限公司、北京畅娱科技有限公司、花生未来（广州）科技有限公司、上海优恒酒店管理有限公司、上海格平信息科技有限公司、中山市自定易网络科技有限公司、用友网络科技股份有限公司、广州市粤企网络科技有限公司、北京东云创达科技有限公司、晋城优逸网络技术有限公司、广东布恩网络有限公司、帝国软件、逍遥 B2C 商城系统、施耐德（Schneider Electric）、zzz 中文网、通达 CMS、海洋 CMS、ZZCMS、YCCMS、UCMS、

BEESCMS、The Apache Software Foundation、SeaCMS、Wdlinux、Bludit、Bo-Blog Wind 和 PHPEMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、深信服科技股份有限公司、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、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。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、河南灵创电子科技有限公司、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、吉林谛听信息技术有限公司、北京禹宏信安科技有限公司、河南信安世纪科技有限公司、北京天地和兴科技有限公司、山东道普测评技术有限公司、北京安华金和科技有限公司、广州三零卫士信息安全有限公司、广州安亿信软件科技有限公司、广东安创信息科技开发有限公司、京东云安全、泽鹿安全、安徽长泰信息安全服务有限公司、北京长亭科技有限公司、浙江鹏信信息科技股份有限公司、赛尔网络有限公司山东分公司、广西网信信息技术有限公司、河北千诚电子科技有限公司、杭州安信检测技术有限公司、上海观安信息技术股份有限公司、浙江安腾信息技术有限公司、上海纽盾科技股份有限公司、武汉绿色网络信息服务有限责任公司、北京智游网安科技有限公司及其他个人白帽子向 CNVD 提交了 2739 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 1385 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）	659	659
北京神州绿盟科技有限公司	548	5
上海交大	389	389
奇安信网神（补天平台）	337	337
深信服科技股份有限公司	222	0
北京天融信网络安全技术有限公司	180	16
哈尔滨安天科技集团股份有限公司	124	0
新华三技术有限公司	99	0

北京数字观星科技有限公司	82	0
华为技术有限公司	67	0
中国电信集团系统集成有限责任公司	40	40
北京启明星辰信息安全技术有限公司	33	21
北京奇虎科技有限公司	20	9
北京知道创宇信息技术股份有限公司	8	0
卫士通信息产业股份有限公司	2	2
北京安信天行科技有限公司	2	2
国瑞数码零点实验室	172	172
北京云科安信科技有限公司	111	111
远江盛邦（北京）网络安全科技股份有限公司	104	104
北京华云安信息技术有限公司	97	97
长春嘉诚信息技术股份有限公司	93	93
杭州迪普科技股份有限公司	54	0
山东新潮信息技术有限公司	39	39
山东华鲁科技发展股份有限公司	38	38
河南灵创电子科技有限公司	27	27
南京众智维信息科技有限公司	14	14
山东云天安全技术有限公司	12	12
吉林谛听信息技术有限公司	12	12
北京禹宏信安科技有限公司	11	11
河南信安世纪科技有限公司	10	10

北京天地和兴科技有限公司	10	10
山东道普测评技术有限公司	8	8
北京安华金和科技有限公司	7	7
广州三零卫士信息安全有限公司	6	6
广州安亿信软件科技有限公司	5	5
广东安创信息科技开发有限公司	3	3
京东云安全	3	3
泽鹿安全	3	3
安徽长泰信息安全服务有限公司	3	3
北京长亭科技有限公司	2	2
浙江鹏信信息科技股份有限公司	1	1
赛尔网络有限公司山东分公司	1	1
广西网信信息技术有限公司	1	1
河北千诚电子科技有限公司	1	1
杭州安信检测技术有限公司	1	1
上海观安信息技术股份有限公司	1	1
浙江安腾信息技术有限公司	1	1
上海纽盾科技股份有限公司	1	1
武汉绿色网络信息服务有限责任公司	1	1
北京智游网安科技有限公司	1	1
CNCERT 宁夏分中心	8	8
CNCERT 青海分中心	4	4

CNCERT 贵州分中心	3	3
CNCERT 安徽分中心	2	2
CNCERT 河北分中心	2	2
个人	440	440
报送总计	4125	2739

本周漏洞按类型和厂商统计

本周，CNVD 收录了 292 个漏洞。应用程序 135 个，WEB 应用 95 个，操作系统 39 个，网络设备（交换机、路由器等网络端设备）21 个，安全产品 1 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	135
WEB 应用	95
操作系统	39
网络设备（交换机、路由器等网络端设备）	21
安全产品	1
数据库	1

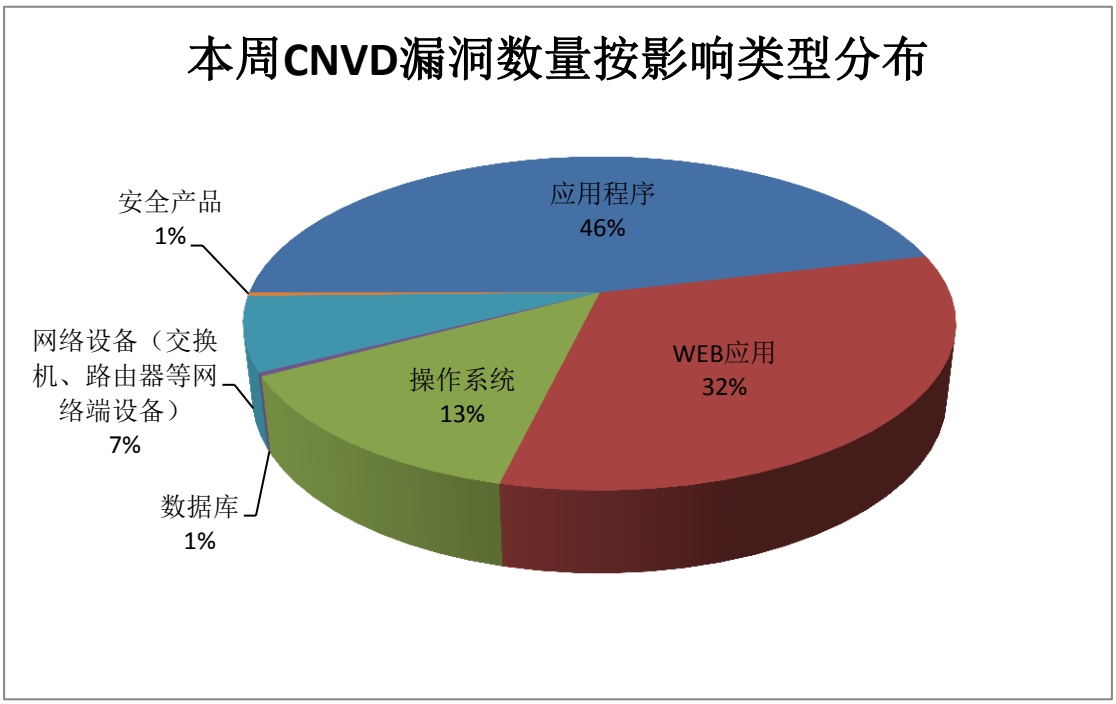

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Google、Microsoft 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	Oracle	59	20%
2	Google	24	8%
3	Microsoft	20	7%
4	CentOS Web Panel（CWP）	15	5%
5	Adobe	13	5%
6	Cisco	11	4%
7	NETGEAR	9	3%
8	Apple	6	2%
9	Mida Solutions	6	2%
10	其他	129	44%

本周行业漏洞收录情况

本周，CNVD 收录了 18 个电信行业漏洞，21 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Apple iOS 和 iPadOS WiFi 组件代码问题漏洞、Google Android External Memory Interface 权限提升漏洞、Cisco Data Center Network Manager 参数注入漏洞、Open-Xchange OX App Suite 访问控制错误漏洞（CNVD-2020-43160）、D-Link DIR-816L 命令注入漏洞”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/

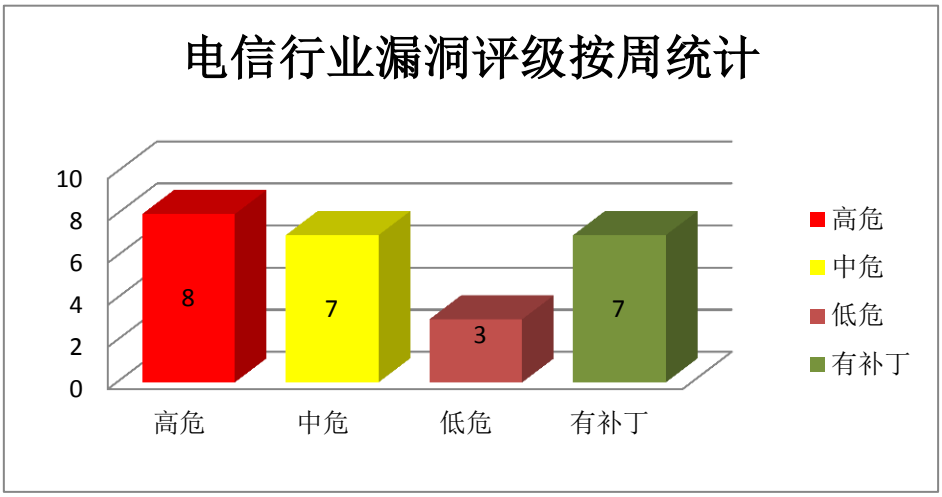

图 3 电信行业漏洞统计

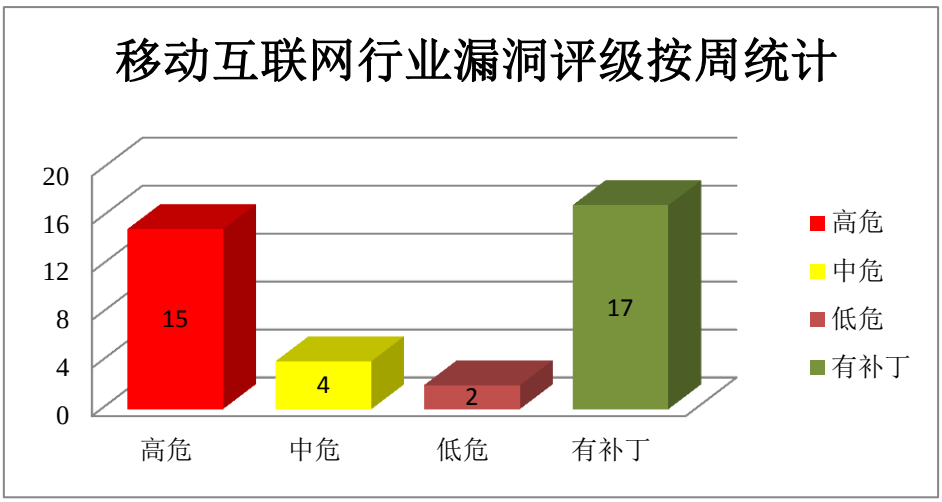

图 4 移动互联网行业漏洞统计

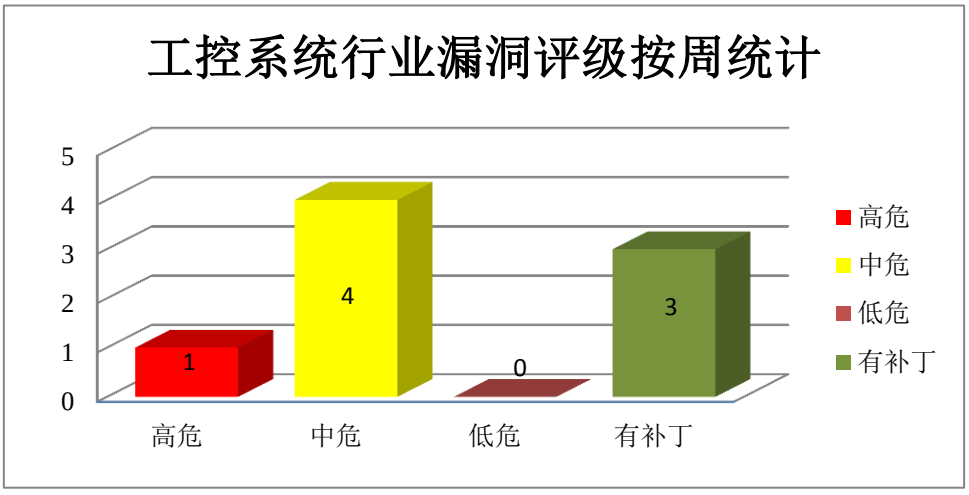

图 5 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco SD-WAN vManage Software 是一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。Cisco Data Center Network Manager（DCNM）是一套数据中心管理系统。Cisco SD-WAN Solution 是一套网络扩展解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取或修改系统上的任意文件，以 root 用户权限登录账户，执行任意命令，导致系统内存耗尽（拒绝服务）等。

CNVD 收录的相关漏洞包括：Cisco SD-WAN vManage Software SQL 注入漏洞（CNVD-2020-42256）、Cisco SD-WAN vManage Software 资源管理错误漏洞、Cisco SD-WAN vManage Software 路径遍历漏洞、Cisco SD-WAN vManage Software 授权问题漏洞、Cisco SD-WAN vManage Software 路径遍历漏洞（CNVD-2020-42258）、Cisco Data Center Network Manager 参数注入漏洞、Cisco SD-WAN Solution 权限许可和访问控制问题漏洞（CNVD-2020-42261）、Cisco SD-WAN Solution 缓冲区溢出漏洞。其中，除“Cisco SD-WAN vManage Software 授权问题漏洞、Cisco Data Center Network Manager 参数注入漏洞、Cisco SD-WAN Solution 权限许可和访问控制问题漏洞（CNVD-2020-42261）、Cisco SD-WAN Solution 缓冲区溢出漏洞”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-2020-42256
https://www.cnvd.org.cn/flaw/show/CNVD-2020-42255
https://www.cnvd.org.cn/flaw/show/CNVD-2020-42260
https://www.cnvd.org.cn/flaw/show/CNVD-2020-42259
https://www.cnvd.org.cn/flaw/show/CNVD-2020-42258
https://www.cnvd.org.cn/flaw/show/CNVD-2020-42257
https://www.cnvd.org.cn/flaw/show/CNVD-2020-42261
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43668

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权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Microsoft Windows WalletService 权限提升漏洞（CNVD-2020-43094、CNVD-2020-43098、CNVD-2020-43096）、Microsoft Windows Delivery Optimization service 权限提升漏洞、Microsoft Windows Modules Installer 权限提升漏洞、Microsoft Windows Update Stack 权限提升漏洞、Microsoft Windows Profile Service 权限提升漏洞、Microsoft Windows psmsrv.dll 权限提升漏洞。其中，“Microsoft Win

dows Update Stack 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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-43094
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43098
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43096
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43101
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43100
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43099
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43105
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43110

3、Adobe 产品安全漏洞

Adobe Bridge 是一款免费数字资产管理应用程序。Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。本周，上述产品被披露存在越界读取和越界写入漏洞，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 Photoshop 越界写入漏洞（CNVD-2020-43379、CNVD-2020-43378、CNVD-2020-43380）、Adobe Photoshop 越界读取漏洞（CNVD-2020-43381、CNVD-2020-43382）、Adobe Bridge 越界写入漏洞（CNVD-2020-43384、CNVD-2020-43383）、Adobe Bridge 越界读取漏洞（CNVD-2020-43385）。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-2020-43379
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43378
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43381
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43380
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43382
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43384
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43383
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43385

4、Google 产品安全漏洞

Chrome 是由 Google 开发的一款 Web 浏览工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息，执行任意代码或造成应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Chrome 信息泄漏漏洞（CNVD-2020-43474、CNVD-2020-43484）、Google Chrome 类型混淆漏洞（CNVD-2020-43473、CNVD-2020-

43483）、Google Chrome WebRTC 输入验证错误漏洞、Google Chrome 缓冲区溢出漏洞（CNVD-2020-43482、CNVD-2020-43485）、Google Chrome 释放后重用漏洞（CNVD-2020-43480）。其中，“Google Chrome 缓冲区溢出漏洞（CNVD-2020-43482）、Google Chrome 释放后重用漏洞（CNVD-2020-43480）、Google Chrome 类型混淆漏洞（CNVD-2020-43483）”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-2020-43474
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43473
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43476
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43482
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43480
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43484
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43483
https://www.cnvd.org.cn/flaw/show/CNVD-2020-43485

5、NETGEAR R6700 缓冲区溢出漏洞（CNVD-2020-43667）

NETGEAR R6700 是一款无线路由器。本周，NETGEAR R6700 被披露存在缓冲区溢出漏洞。该漏洞源于程序将用户提供的数据复制到基于栈的固定缓冲区之前，未能正确验证数据长度。攻击者可利用该漏洞绕过身份验证。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-2020-43667

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-2020-42654	Citrix Systems Workspace App 访问控制错误漏洞（CNVD-2020-42654）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.citrix.com/article/CTX277662
CNVD-2020-42655	D-Link DIR-816L 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10169
CNVD-2020-43130	Pillow PCX P 模式缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://pillow.readthedocs.io/en/stable/releasenotes/6.2.2.html

CNVD-2020-43153	IBM Security Key Lifecycle Manager 账户管理漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/6253781
CNVD-2020-43160	Open-Xchange OX App Suite 访问控制错误漏洞（CNVD-2020-43160）	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.open-xchange.com/
CNVD-2020-43605	Red Hat AMQ Online 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://access.redhat.com/errata/RHSA-2020:3209
CNVD-2020-43617	TYPO3 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://typo3.org/security/advisory/typo3-psa-2020-001/
CNVD-2020-43619	Artifex Software Ghostscript 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://artifex.com/security-advisories/CVE-2020-15900
CNVD-2020-43618	Dell EMC OpenManage Server Administrator 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://www.dell.com/support/article/zh-cn/sln322304/dsa-2020-172-dell-emc-openmanage-server-administrator-omsa-path-traversal-vulnerability
CNVD-2020-43664	HMS Networks eCatcher 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://ewon.biz/technical-support/pages/all-downloads

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞读取或修改系统上的任意文件，以 root 用户权限登录账户，执行任意命令，导致系统内存耗尽（拒绝服务）等。此外，Microsoft、Adobe、Google 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，绕过安全限制，获取敏感信息，执行任意代码或造成应用程序崩溃等。另外，NETGEAR R6700 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞绕过身份验证。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、eGroupWare 'spellchecker.php'远程代码执行漏洞

验证描述

eGroupWare 是一个多用户，在以 PHP 为基础的 API 上的定制集为基础开发的，以 WEB 为基础的工作件套装。

eGroupWare 'spellchecker.php'存在远程代码执行漏洞，该漏洞源于程序未能正确地验证用户提交的数据。远程攻击者可通过发送恶意的请求利用该漏洞在底层操作系统上执行任意代码。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35891

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-43466

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. WordPress 插件中的关键安全漏洞允许远程代码执行

研究人员警告称，WordPress 的插件 Comments – wpDiscuz 中存在一个严重漏洞，该漏洞使未经身份验证的攻击者可以上传任意文件(包括 PHP 文件)，并最终在易受攻击的网站服务器上执行远程代码。

参考链接：https://threatpost.com/critical-rce-flaw-wordpress-plugin-on-70k-sites/157824/

2. 严重 GRUB2 Bootloader 漏洞影响数十亿 Linux 和 Windows 系统

大部分 Linux 系统使用的几乎所有 GRUB2 bootloader 签名版本中存在一个严重的安全漏洞。成功利用该漏洞，威胁行为者可以入侵操作系统的启动过程，即便 Secure Boot 验证机制处于活动状态。该漏洞被贴切地命名为 BootHole，允许在 GRUB bootloader 中执行任意代码。攻击者可利用该漏洞在操作系统之前加载被称为 bootkit 的恶意软件。以此种方式入侵系统授予该恶意软件最高的权限，并使得该恶意软件实际上无法被检测到，因为当操作系统上的安全解决方案启动时，该恶意软件已经在运行了。

参考链接：https://www.freebuf.com/vuls/245013.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