国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 08 月 17 日-2020 年 08 月 23 日　　2020 年第 34 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 381 个，其中高危漏洞 135 个、中危漏洞 202 个、低危漏洞 44 个。漏洞平均分值为 5.91。本周收录的漏洞中，涉及 0day 漏洞 151 个（占 40%），其中互联网上出现“vBulletin 跨站脚本漏洞、vsftpd 操作系统命令注入漏洞”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 3061 个，与上周（3721 个）环比减少 18%。

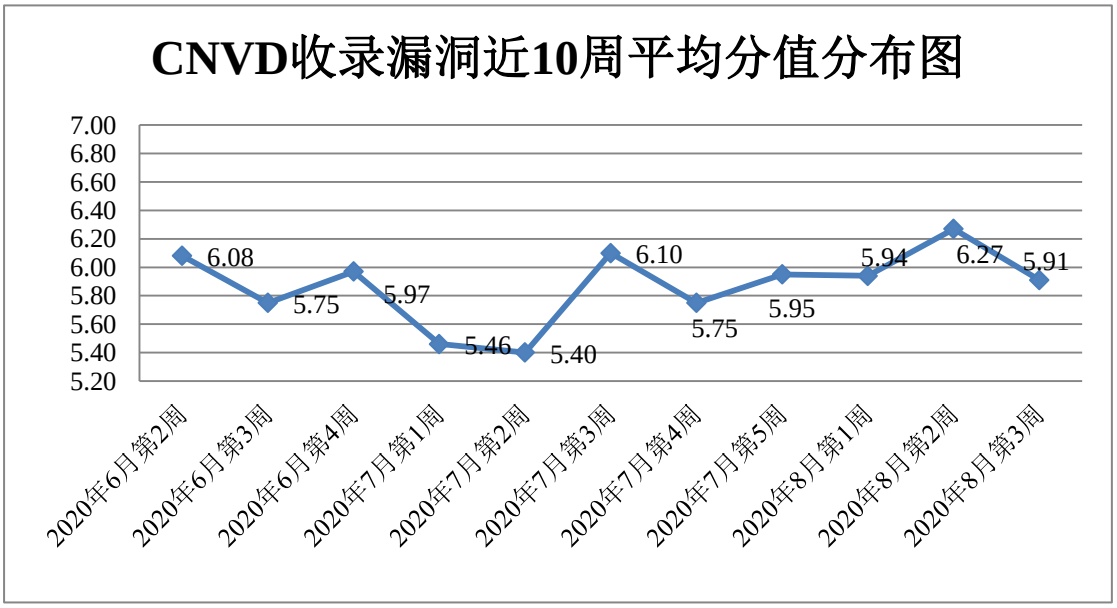

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 9 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 304 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 43 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 22 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：

汉中启元动力网络有限公司、深圳市华磊信息科技有限公司、北京中成科信科技发展有限公司、成都新线加科技有限公司、深圳市瑞博龙科技开发有限公司、青岛易企天创管理咨询有限公司、北京良精志诚科技有限责任公司、武汉贝云网络科技有限公司、嘉兴想天信息科技有限公司、赤峰易拓网络有限公司、深圳警翼智能科技股份有限公司、校无忧科技网络公司、北京灵州网络技术有限公司、烽火通信科技股份有限公司、北京小米科技有限责任公司、广州市问途信息技术有限公司、天信仪表集团有限公司、安徽希望网络科技有限公司、合肥奇乐网络科技有限公司、北京通达信科科技有限公司、小米科技有限责任公司、洪湖尔创网联信息技术有限公司、南洋天融信科技集团股份有限公司、通用电气（GE）公司、深圳市微客互动有限公司、北京汇东科技有限公司、上海卓岚信息科技有限公司、研华科技（中国）有限公司、上海装盟信息科技有限公司、诸城市三剑网络传媒有限公司、上海智休信息科技有限公司、润申信息科技(上海)有限公司、哈尔滨伟成科技有限公司、北京正影网络科技有限公司、深圳市点晴信息技术有限公司、广州巨腾信息科技有限公司、深圳市汇川技术股份有限公司、金山软件股份有限公司、湖南翱云网络科技有限公司、北京通达志成科技有限公司、无锡众思宸网络科技有限公司、西安佰联网络技术有限公司、西安知先信息技术有限公司、武汉微问网络科技有限公司、浙江兴旺宝明通网络有限公司、成都智蜂网科技有限责任公司、用友网络科技股份有限公司、新韩进出口有限公司、合肥诚商信息科技有限公司、上海有品网络科技有限公司、山东领图信息科技股份有限公司、深圳市天视通电子科技有限公司、宜兴易发网络服务有限公司、上海商派网络科技有限公司、昆山优网信息科技有限公司、友讯科技、校无忧科技、上海荃路软件开发工作室、飞飞影视导航系统、易天网络、Heybbs 微社区、逍遥 B2C 商城系统、YzmCMS、115CMS、Heybbs、MYUCMS、YCCMS 和 Code Industry Ltd。

本周，CNVD 发布了《关于深信服终端检测平台（EDR）存在远程命令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/5677

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京神州绿盟科技有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、深信服科技股份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、远江盛邦（北京）网络安全科技股份有限公司、山东新潮信息技

术有限公司、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、杭州迪普科技股份有限公司、山东云天安全技术有限公司、安徽长泰信息安全服务有限公司、南京众智维信息科技有限公司、北京天地和兴科技有限公司、博智安全科技股份有限公司、山东道普测评技术有限公司、杭州海康威视数字技术股份有限公司、平安银河实验室、国家互联网应急中心、上海犀点意象网络科技有限公司、河北千诚电子科技有限公司、上海观安信息技术股份有限公司、北京卓识网安技术股份有限公司、中国工商银行、河南信安世纪科技有限公司、四川哨兵信息科技有限公司、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 3061 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 1990 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）	1404	1404
上海交大	586	586
哈尔滨安天科技集团股份有限公司	234	0
北京神州绿盟科技有限公司	209	13
华为技术有限公司	156	0
北京天融信网络安全技术有限公司	135	1
深信服科技股份有限公司	84	2
北京启明星辰信息安全技术有限公司	77	0
新华三技术有限公司	71	0
中国电信集团系统集成有限责任公司	63	63
西安四叶草信息技术有限公司	28	28
北京安信天行科技有限公司	20	20
浙江大华技术股份有限公司	10	10
北京知道创宇信息技术股份有限公司	4	0
国瑞数码零点实验室	220	220

山东华鲁科技发展股份有限公司	90	90
远江盛邦（北京）网络安全科技股份有限公司	59	59
山东新潮信息技术有限公司	47	47
北京华云安信息技术有限公司	29	29
河南灵创电子科技有限公司	23	23
杭州迪普科技股份有限公司	15	0
山东云天安全技术有限公司	10	10
安徽长泰信息安全服务有限公司	9	9
南京众智维信息科技有限公司	8	8
北京天地和兴科技有限公司	7	7
博智安全科技股份有限公司	7	7
山东道普测评技术有限公司	6	6
杭州海康威视数字技术股份有限公司	5	5
平安银河实验室	4	4
国家互联网应急中心	3	3
上海犀点意象网络科技有限公司	2	2
河北千诚电子科技有限公司	2	2
上海观安信息技术股份有限公司	2	2
北京卓识网安技术股份有限公司	2	2
中国工商银行	1	1
河南信安世纪科技有限公司	1	1
四川哨兵信息科技有限公司	1	1

北京智游网安科技有限公司	1	1
CNCERT 海南分中心	4	4
CNCERT 青海分中心	1	1
CNCERT 河南分中心	1	1
CNCERT 广西分中心	1	1
个人	388	388
报送总计	4030	3061

本周漏洞按类型和厂商统计

本周，CNVD 收录了 381 个漏洞。应用程序 189 个，WEB 应用 124 个，操作系统 28 个，网络设备（交换机、路由器等网络端设备）18 个，智能设备（物联网终端设备）13 个，安全产品 9 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	189
WEB 应用	124
操作系统	28
网络设备（交换机、路由器等网络端设备）	18
智能设备（物联网终端设备）	13
安全产品	9

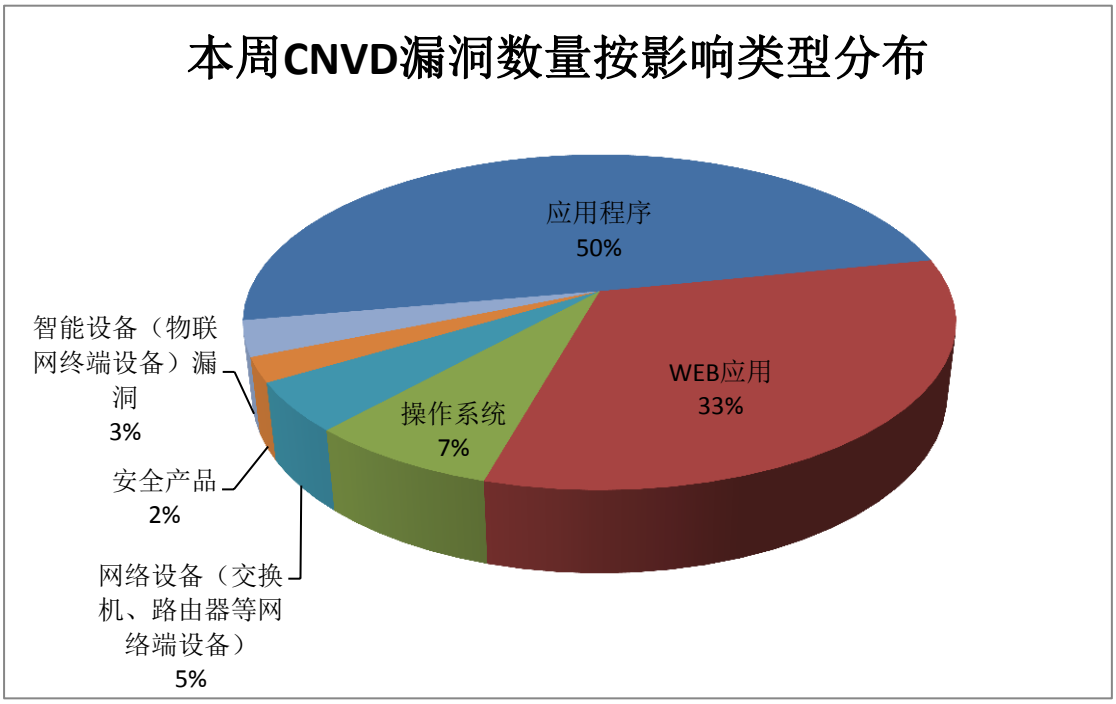

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Huawei、Microsoft、Red Hat 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	Huawei	22	6%
2	Microsoft	16	4%
3	Red Hat	15	4%
4	IBM	15	4%
5	Mozilla	13	3%
6	Google	12	3%
7	Marvell	10	3%
8	JetBrains	8	2%
9	Schneider Electric	7	2%
10	其他	263	69%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，26 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Marvell QConvergeConsole 远程代码执行漏洞、Google Android Kernel Audio 组件缓冲区溢出漏洞、多款 Mitsubishi Electric 产品访问控制错误

漏洞、Schneider Electric APC Easy UPS On-Line SoundUploadServlet 路径遍历漏洞”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/

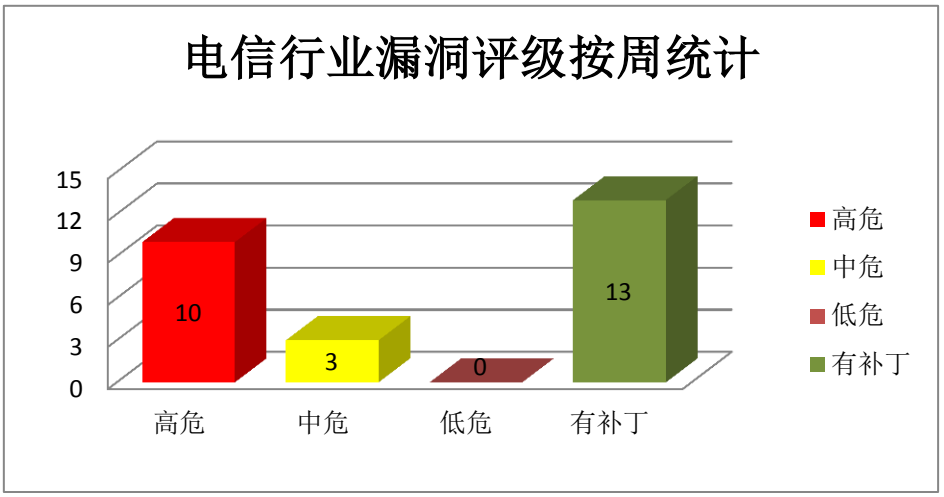

图 3 电信行业漏洞统计

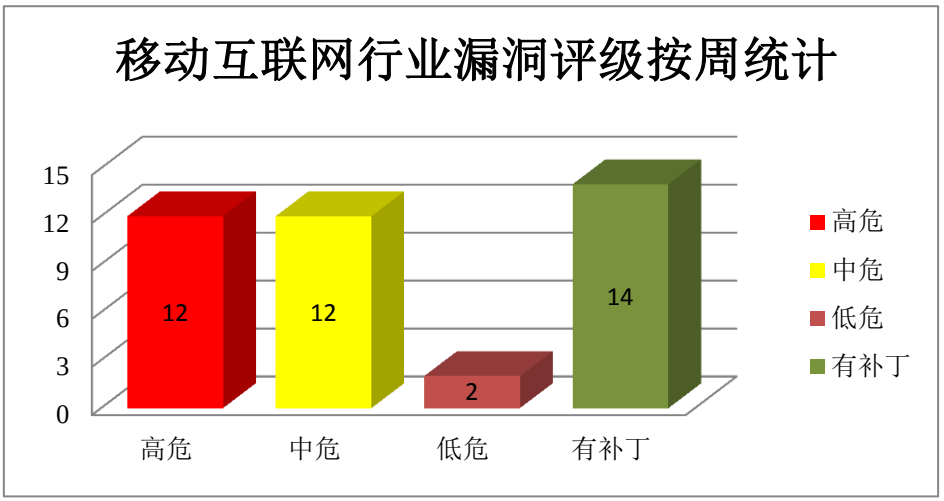

图 4 移动互联网行业漏洞统计

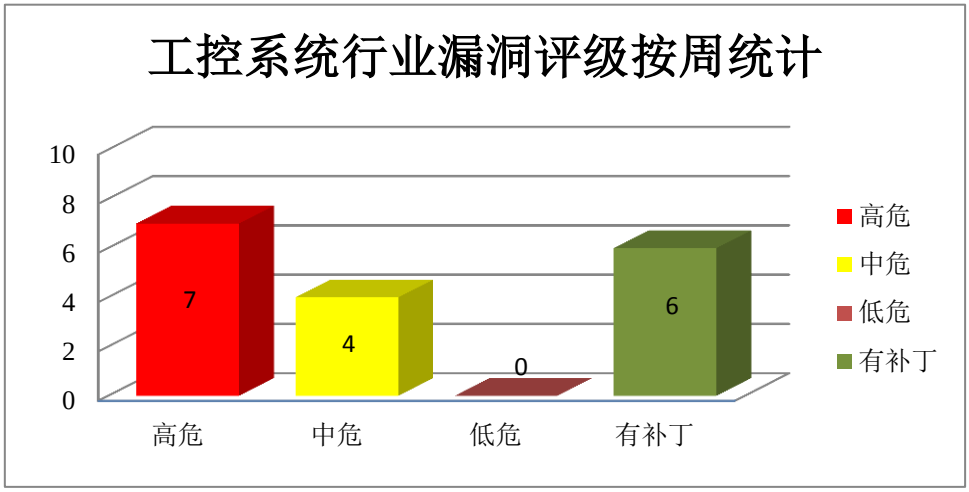

图 5 工控系统行业漏洞统计

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、 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。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，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Framework 权限绕过漏洞（CNVD-2020-46320、CNVD-2020-46323、CNVD-2020-46321）、Google Android Media Framework 越界读取漏洞（CNVD-2020-46322、CNVD-2020-46324）、Google Android Kernel Audio 组件缓冲区溢出漏洞、Google Android Kernel Audio 组件权限提升漏洞、Google Android Media Framework 越界写入漏洞（CNVD-2020-46325）。其中，“Google Android Kernel Audio 组件缓冲区溢出漏洞、Google Android Kernel Audio 组件权限提升漏洞”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-2020-46320

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46323

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46322

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46321

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46327

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46326

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46325

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46324

2、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取本地文件，修改文件扩展，执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2020-46331、CNVD-2020-46338）、Mozilla Firefox 输入验证错误漏洞（CNVD-2020-46333）、Mozilla Firefox 代码问题漏洞（CNVD-2020-46337、CNVD-2020-46339）、Mozilla Firefox 产品认证绕过漏洞、Mozilla Firefox 路径遍历漏洞、Mozilla Firefox 安全限制绕过漏洞（CNVD-2020-46451）。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-2020-46331

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46333

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46337

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46336

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46334

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46338

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46339

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46451

3、Huawei 产品安全漏洞

Huawei FusionCompute 是中国华为（Huawei）公司的一款计算机虚拟化引擎。Huawei Mate 30 是一款智能手机。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信息，提升权限，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei FusionCompute 命令注入漏洞、Huawei FusionCompute 设计不当漏洞、Huawei FusionCompute 信息泄露漏洞（CNVD-2020-46462、CNVD-2020-46464、CNVD-2020-47548）、Huawei Mate 30 拒绝服务漏洞、Huawei FusionCompute 授权问题漏洞、Huawei FusionCompute 本地权限提升漏洞。其中，“Huawei FusionCompute 命令注入漏洞、Huawei FusionCompute 设计不当漏洞”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-2020-46458

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46457

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46462

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46460

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46466

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46465

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46464

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47548

4、Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Edge 是一款 Windows 10 之后版本系统附带的 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，损坏内存等。

CNVD 收录的相关漏洞包括：Microsoft Windows Graphics Components 远程代码执行漏洞（CNVD-2020-46637）、Microsoft Windows Kernel 权限提升漏洞（CNVD-2020-46636）、Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2020-46639、CNVD-2020-46643）、Microsoft Windows State Repository Service 权限提升漏洞（CNVD-2020-46640、CNVD-2020-46641、CNVD-2020-46642）、Microsoft Edge 代码执行漏洞（CNVD-2020-46810）。其中，“Microsoft Windows Graphics Components 远程代码执行漏洞（CNVD-2020-46637）、Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2020-46639、CNVD-2020-46643）、Microsoft Edge 代码执行漏洞（CNVD-2020-46810）”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-2020-46637

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46636

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46639

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46641

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46640

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46643

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46642

https://www.cnvd.org.cn/flaw/show/CNVD-2020-46810

5、Red Hat libvirt 权限提升漏洞

Red Hat libvirt 是美国红帽（Red Hat）公司的一个用于实现 Linux 虚拟化功能的 Linux API，它支持各种 Hypervisor，包括 Xen 和 KVM，以及 QEMU 和用于其他操作系统的一些虚拟产品。本周，Red Hat libvirt 被披露存在权限提升漏洞。攻击者可利用该漏洞访问 libvirt 并提升权限。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-2020-47593

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-2020-46349	Marvell QConvergeConsole 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.marvell.com/content/dam/marvell/en/public-collateral/fibre-channel/marvell-fibre-channel-security-advisory-2020-07.pdf
CNVD-2020-46486	GitLab 内存耗尽漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://about.gitlab.com/releases/2020/08/05/gitlab-13-2-3-released/
CNVD-2020-46552	深信服终端监测响应平台（EDR）远程命令执行漏洞	高	深信服官方已发布更新版本和补丁，建议相关用户尽快升级至 3.2.21 版本或升级补丁修复漏洞：https://www.sangfor.com.cn/product/net-safe-mobile-security-edr.html
CNVD-2020-46554	TP-Link TL-PS310U 认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tp-link.com/us/home-networking/print-server/tl-ps310u/
CNVD-2020-46579	Apache Shiro 权限绕过漏洞	高	目前官方已发布漏洞修复版本，建议用户下载使用：https://lists.apache.org/thread.html/r539f87706094e79c5da0826030384373f00410689369128768568 35f%40%3Cdev.shiro.apache.org%3E
CNVD-2020-46808	SAP NetWeaver Knowledge Management 跨站脚本漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552603345
CNVD-2020-46816	ZOHO ManageEngine ADSelfService Plus 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，补丁获取链接： https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6003-release-faceid-support
CNVD-2020-46825	TYPO3 wec_discussion extension 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://typo3.org/security/advisory/typo3-sa-2011-003/
CNVD-2020-46854	Parallels Desktop 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://kb.parallels.com/en/125013

CNVD-2020-47036	Lenovo Service Bridge 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://support.lenovo.com/us/zh/solutions/len-27725

小结：本周，Google 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，提升权限，执行任意代码。此外，Mozilla、Huawei、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取信息，提升权限，执行任意代码，导致拒绝服务等。另外，Red Hat libvirt 被披露存在权限提升漏洞。攻击者可利用该漏洞访问 libvirt 并提升权限。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、vBulletin 跨站脚本漏洞

验证描述

vBulletin 是美国 InternetBrands 和 vBulletinSolutions 公司的一款基于 PHP 和 MySQL 的开源 Web 论坛程序。

vBulletin 5.x 版本中存在跨站脚本漏洞，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代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/158866/vBulletin-5.x-Remote-Code-Execution.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-47041

信息提供者

新华三技术有限公司

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. PHP 8 Beta 2 发布，修复一个内存泄漏 bug

PHP 8 Beta 2 已经发布，自从进入 Beta 阶段，PHP 8 已进入特性冻结期，不会有特性上的变更。此版本修复了一个 SPL bug：由于缺少 zend_restore_error_handling() 而导致 SplFileInfo 中的内存泄漏。

参考链接：https://www.cnbeta.com/articles/tech/1018927.htm

2. Google 服务全球性故障

Google 旗下多项服务出现异常，包括 Gmail、Google Drive、Google 文件、Google Meet、Google Voice 的服务出现中断，随后，Google 表示原因是亚特兰大的路由器故障。

参考链接：https://www.zdnet.com/article/google-suffers-global-outage-affecting-gmail-and-many-g-suite-services/

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