国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 10 月 19 日-2020 年 10 月 25 日　　2020 年第 43 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 597 个，其中高危漏洞 235 个、中危漏洞 286 个、低危漏洞 76 个。漏洞平均分值为 6.20。本周收录的漏洞中，涉及 0day 漏洞 341 个（占 57%），其中互联网上出现“MonoCMS Blog 信息泄露漏洞、CMS Made Simple 跨站脚本漏洞（CNVD-2020-57873）”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 12085 个，与上周（5332 个）环比增加 1.27 倍。

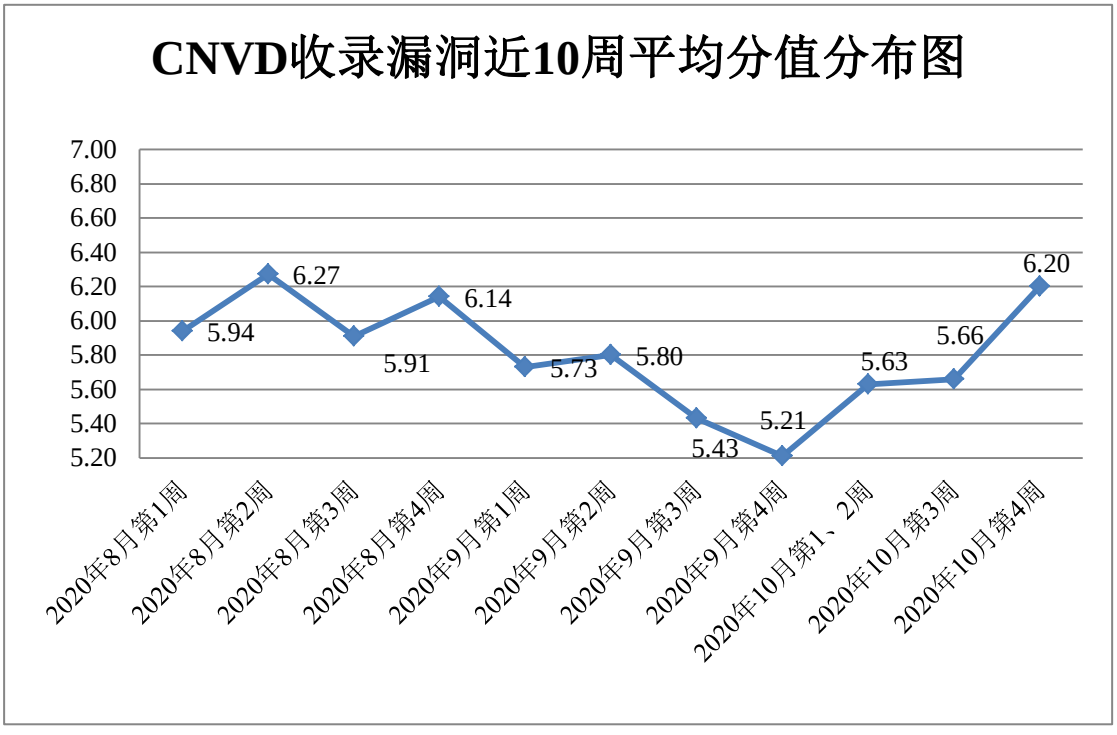

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 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 513 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 91 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 25 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：

深圳市迪元素科技有限公司、小米科技有限责任公司、深圳市迅雷网文化有限公司、长沙米拓信息技术有限公司、长春市南北科技有限公司、甲骨文股份有限公司、厦门悦讯信息科技股份有限公司、北京粉笔蓝天科技有限公司、北京飞书科技有限公司、深圳齐心好视通云计算有限公司、北京百家互联科技有限公司、同方知网技术有限公司、河南礼恰网络科技有限公司、苏州思杰马克丁软件有限公司、北京我知科技有限公司、湖南潭州教育网络科技有限公司、大庆紫金桥软件技术有限公司、天津迅读科技有限公司、新乡市落笔千言网络技术有限公司、梅州海能科技有限公司、南京云恩通讯科技有限公司、深圳市邦明科技有限公司、杭州惊鹊网络科技有限公司、上海数字世纪网络有限公司、湖南星云网络科技有限公司、武汉良师在线教育科技有限公司、西安九佳易信息资讯有限公司、大汉软件股份有限公司、北京九州云腾科技有限公司、欧姆龙（中国）有限公司、深圳市科荣软件股份有限公司、深圳乐播科技有限公司、广东天宸网络科技有限公司、华硕电脑（上海）有限公司、上海护盾信息科技有限公司、上海硬通网络科技有限公司、广州市政务服务数据管理局、上海惠诚咨询有限公司、茉柏枘（上海）软件科技有限公司、用友网络科技股份有限公司、广州市保伦电子有限公司、北京通达信科科技有限公司、上海易正信息技术有限公司、江苏倢科软件有限公司、合肥启迈网络科技有限公司、西安昊博智能科技有限公司、云南天人网络科技有限公司、长沙友点软件科技有限公司、福州网钛软件科技有限公司、深圳市龙艺脉网络科技有限公司、北京国炬信息技术有限公司、瑞芯微电子股份有限公司、研华科技（中国）有限公司、浙江创源环境科技股份有限公司、北京意畅科技股份有限公司、利凌公司、中国华冶科工集团有限公司、安徽环美智能科技有限公司、北京东云创达科技有限公司、北京文网亿联科技有限公司、杭州艾朴软件有限公司、广东小天才科技有限公司、广联达科技股份有限公司、同方知网（北京）技术有限公司、北京灯果网络科技有限公司、哈尔滨中龙百盈科技开发有限公司、深圳点猫科技有限公司、北京世纪好未来教育科技有限公司、广州视睿电子科技有限公司、山东力创科技股份有限公司、上海晟央网络科技有限公司、深圳市马博科技有限公司、厦门海为科技有限公司、北京和利时系统工程有限公司、黄石市科威自控有限公司、厦门印了么信息科技股份有限公司、青岛易企天创管理咨询有限公司、稻草人 CMS、鱼跃 cms、Yycms、HadSky、KKCMS、Schneider Electric、115CMS、XiaoCms、zzcms、Shop7z、UCMS、SeaCMS 和 ThinkAdmin。

本周，CNVD 发布了《Oracle 发布 2020 年 10 月的安全公告》。详情参见 CNVD 网站公

告内容。

https://www.cnvd.org.cn/webinfo/show/5788

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、华为技术有限公司、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。长春嘉诚信息技术股份有限公司、山东华鲁科技发展股份有限公司、西安交大捷普网络科技有限公司、北京华云安信息技术有限公司、北京天地和兴、河南灵创电子科技有限公司 、北京顶象技术有限公司、杭州迪普科技股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、京东云安全、山东新潮信息技术有限公司、河南信安世纪科技有限公司、北京长亭科技有限公司、北京机沃科技有限公司、吉林谛听信息技术有限公司、国瑞数码零点实验室、上海观安信息技术股份有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京零零信安科技有限公司、山石网科通信技术股份有限公司、星云博创科技有限公司、南京众智维信息科技有限公司、平安银河实验室、山东云天安全技术有限公司、上海纽盾科技股份有限公司、广州市蓝爵计算机科技有限公司、长扬科技（北京）有限公司、北京威努特技术有限公司、广西等保安全测评有限公司、四川哨兵信息科技有限公司、北京智游网安科技有限公司、深圳市魔方安全科技有限公司、西安秦易信息技术有限公司及其他个人白帽子向 CNVD 提交了 13275 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 10988 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
奇安信网神（补天平台）	8413	8413
斗象科技（漏洞盒子）	2148	2148
上海交大	427	427
北京天融信网络安全技术有限公司	259	5
华为技术有限公司	237	0
哈尔滨安天科技集团股份有限公司	211	0
新华三技术有限公司	179	0

北京数字观星科技有限公司	90	0
北京启明星辰信息安全技术有限公司	87	25
北京神州绿盟科技有限公司	86	2
深信服科技股份有限公司	69	0
中国电信集团系统集成有限责任公司	54	54
中新网络信息安全股份有限公司	35	35
北京知道创宇信息技术股份有限公司	4	0
长春嘉诚信息技术股份有限公司	81	81
山东华鲁科技发展股份有限公司	55	55
西安交大捷普网络科技有限公司	50	50
北京华云安信息技术有限公司	46	46
北京天地和兴	36	36
河南灵创电子科技有限公司	26	26
北京顶象技术有限公司	20	20
杭州迪普科技股份有限公司	15	15
北京云科安信科技有限公司（Seraph 安全实验室）	15	15
京东云安全	15	15
山东新潮信息技术有限公司	15	15
河南信安世纪科技有限公司	12	12
北京长亭科技有限公司	11	11
北京机沃科技有限公司	9	9
吉林谛听信息技术有限公司	7	7

国瑞数码零点实验室	6	6
上海观安信息技术股份有限公司	6	6
远江盛邦（北京）网络安全科技股份有限公司	6	6
北京零零信安科技有限公司	5	5
山石网科通信技术股份有限公司	4	4
星云博创科技有限公司	4	4
南京众智维信息科技有限公司	3	3
平安银河实验室	3	3
山东云天安全技术有限公司	3	3
上海纽盾科技股份有限公司	3	3
广州市蓝爵计算机科技有限公司	2	2
长扬科技（北京）有限公司	2	2
北京威努特技术有限公司	2	2
广西等保安全测评有限公司	2	2
四川哨兵信息科技有限公司	2	2
北京智游网安科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
西安秦易信息技术有限公司	1	1
CNCERT 辽宁分中心	4	4
CNCERT 四川分中心	3	3
CNCERT 河北分中心	1	1
CNCERT 青海分中心	1	1
CNCERT 上海分中心	1	1

个人	497	497
报送总计	13275	12085

本周漏洞按类型和厂商统计

本周，CNVD 收录了 597 个漏洞。应用程序 264 个，WEB 应用 200 个，操作系统 50 个，网络设备（交换机、路由器等网络端设备）35 个，数据库 23 个，智能设备（物联网终端设备）15 个，安全产品 10 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	264
WEB 应用	200
操作系统	50
网络设备（交换机、路由器等网络端设备）	35
数据库	23
智能设备（物联网终端设备）	15
安全产品	10

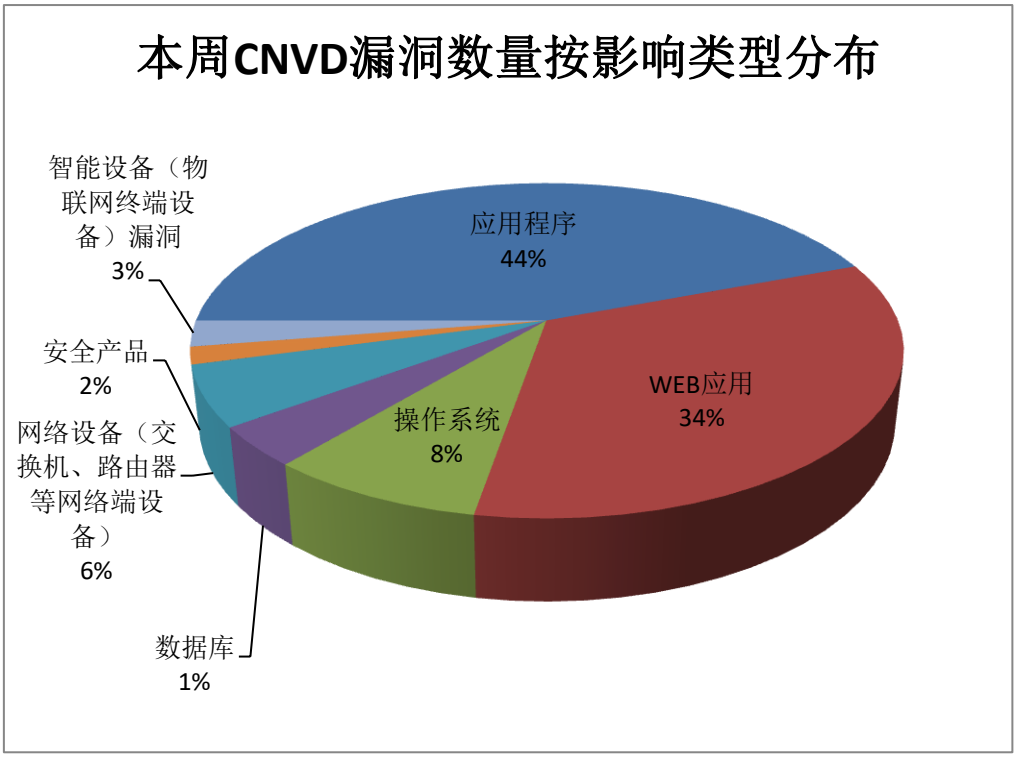

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 HPE、Google、Adobe 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	HPE	43	7%
2	Google	35	6%
3	Adobe	25	4%
4	INFRAWARE	20	3%
5	Oracle	20	3%
6	Microsoft	16	3%
7	研华科技（中国）有限公司	14	2%
8	IBM	12	2%
9	Cisco	11	2%
10	其他	401	68%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，60 个移动互联网行业漏洞，27 个工控行业漏洞（如下图所示）。其中，“Cisco StarOS 权限提升漏洞（CNVD-2020-57576）、Google Android 释放后重用漏洞（CNVD-2020-58104）、Apple iOS 越界写入漏洞、ARC Informatique PcVue 远程代码执行漏洞”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/

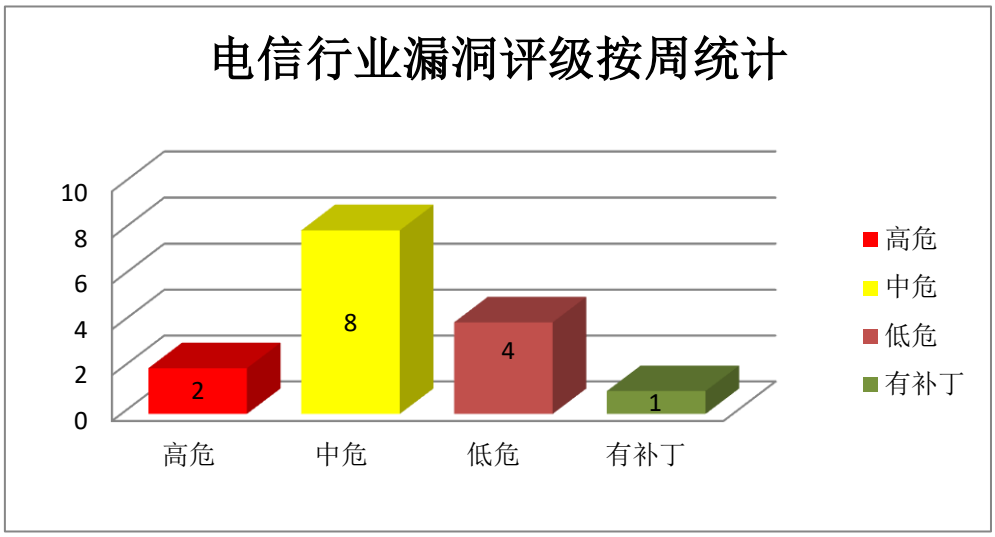

图 3 电信行业漏洞统计

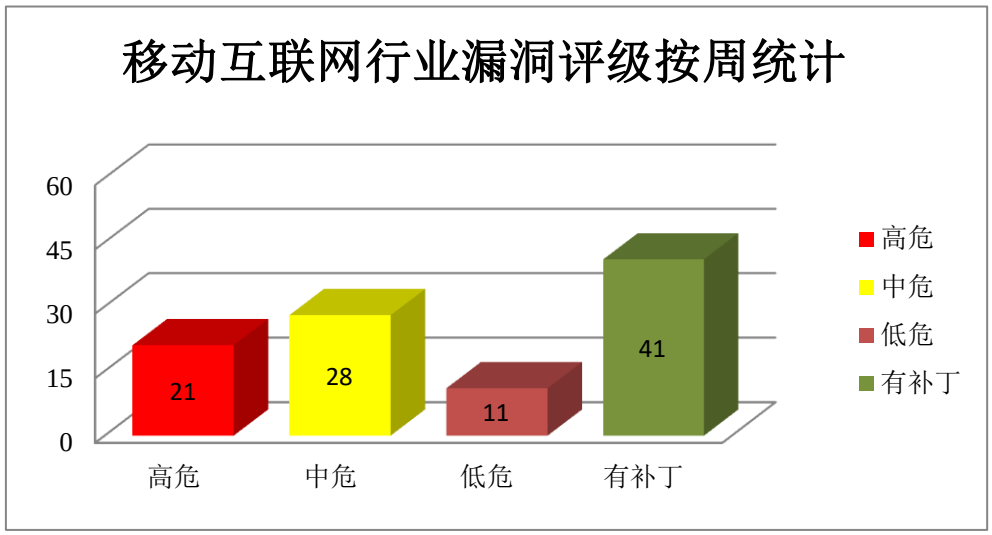

图 4 移动互联网行业漏洞统计

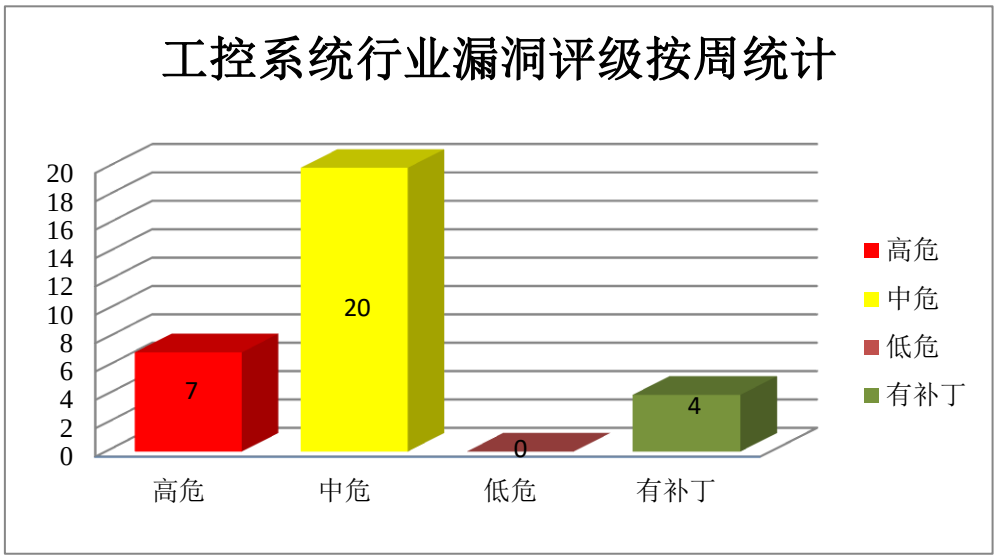

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe InDesign 是 Adobe 公司的一个桌面出版(DTP)的应用程序，主要用于各种印刷品的排版编辑。Adobe After Effects 是美国奥多比（Adobe）公司的一套视觉效果和动态图形制作软件。Adobe Animate 是一款多媒体创作和计算机动画程序。Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。Adobe Magento 是美国奥多比（Adobe）公司的一套开源的 PHP 电子商务系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞实现任意代码执行。

CNVD 收录的相关漏洞包括：Adobe InDesign 内存破坏漏洞（CNVD-2020-57855）、Adobe Animate 越界读取漏洞（CNVD-2020-57863、CNVD-2020-57864）、Adobe Animate 栈缓冲区溢出漏洞、Adobe Animate 双重释放漏洞、Adobe After Effects 越界读取漏洞（CNVD-2020-57860）、Adobe Flash Player 空指针解引用漏洞、Adobe Magento 文件上传列表绕过漏洞。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-2020-57855

https://www.cnvd.org.cn/flaw/show/CNVD-2020-57864

https://www.cnvd.org.cn/flaw/show/CNVD-2020-57863

https://www.cnvd.org.cn/flaw/show/CNVD-2020-57862

https://www.cnvd.org.cn/flaw/show/CNVD-2020-57861

https://www.cnvd.org.cn/flaw/show/CNVD-2020-57860

https://www.cnvd.org.cn/flaw/show/CNVD-2020-57892

https://www.cnvd.org.cn/flaw/show/CNVD-2020-57891

2、Microsoft 产品安全漏洞

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。Microsoft Azure 是一款开放的企业级云计算平台。Windows Server 是微软发布的一系列服务器操作系统的品牌名，它包括所有以“Windows Server”为品牌发布的 Windows 操作系统。Microsoft Visual Studio Code 是美国微软（Microsoft）公司的一款开源的代码编辑器。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，从而进一步入侵用户系统，提交特殊的请求，在未有正确授权的情况下调用 HTTP 功能，导致 DNS 服务无响应等。

CNVD 收录的相关漏洞包括：Microsoft SharePoint 远程代码执行漏洞（CNVD-2020-57589）、Microsoft SharePoint 信息泄露漏洞（CNVD-2020-57588）、Microsoft Azure

特权提升漏洞、Microsoft SharePoint 授权问题漏洞、Microsoft Windows Server 拒绝服务漏洞（CNVD-2020-57795）、Microsoft SharePoint Server 资源管理错误漏洞、Microsoft Windows Server 远程代码执行漏洞（CNVD-2020-57799）、Microsoft Visual Studio Code 代码执行漏洞。其中“Microsoft Azure 特权提升漏洞、Microsoft Visual Studio Code 代码执行漏洞”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-2020-57589
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57588
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57587
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57796
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57795
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57793
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57799
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57802

3、Google 产品安全漏洞

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 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，攻击者可利用漏洞漏洞获取蓝牙服务器相关信息，实现本地权限提升，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android 释放后重用漏洞（CNVD-2020-58104）、Google Android 越界读取漏洞（CNVD-2020-58112）、Google Android 整数溢出漏洞（CNVD-2020-58117）、Google Android Framework 组件权限提升漏洞（CNVD-2020-58120、CNVD-2020-58119）、Google Android system 组件权限提升漏洞（CNVD-2020-58121）、Google Android System 权限提升漏洞（CNVD-2020-58128）、Google Android System 远程代码执行漏洞（CNVD-2020-58132）。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-2020-58104
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58112
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58117
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58120
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58119
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58121
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58128
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58132

4、HPE 产品安全漏洞

HPE Intelligent Management Center (iMC)是美国惠普企业公司（Hewlett Packard Enterprise，HPE）的一套网络智能管理中心解决方案。本周，上述产品被披露存在表达式语言注入远程代码执行漏洞，攻击者可利用漏洞执行远程代码。

CNVD 收录的相关漏洞包括：HPE Intelligent Management Center (iMC) comparefilesresult 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) faultdevparasset 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) eventinfo_content 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) adddevicetoview 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) ictexpertcsvdownload 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) deployselectsoftware 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) deployselectbootrom 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) devgroupselect 表达式语言注入远程代码执行漏洞。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-2020-57961
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57960
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57959
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57958
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57966
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57965
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57964
https://www.cnvd.org.cn/flaw/show/CNVD-2020-57963

5、GetSimpleCMS 路径遍历漏洞

GetSimpleCMS 是个人开发者的一个内容管理系统。本周，GetSimpleCMS 产品被披露存在路径遍历漏洞。攻击者可利用该漏洞删除任意文件。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-2020-57871

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-2020-57568	Foxit Reader 和 PhantomPDF 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：

	（CNVD-2020-57568）		https://www.foxitsoftware.com/support/security-bulletins.html
CNVD-2020-57576	Cisco StarOS 权限提升漏洞（CNVD-2020-57576）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-priv-esc-gGCUMFxv
CNVD-2020-57581	Cisco IOS XE 同意令牌绕过漏洞（CNVD-2020-57581）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ctbypass-7QHAfHkK
CNVD-2020-57822	ARC Informatique PcVue 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://www.pcvuesolutions.com/index.php/support-a-services/resources/security-alerts-95138
CNVD-2020-57828	Sierra Wireless ALEOS 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://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/#sthash.qJHF5imp.dpbs
CNVD-2020-57853	Apple iOS 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://support.apple.com/en-us/HT211850
CNVD-2020-57855	Adobe InDesign 内存破坏漏洞（CNVD-2020-57855）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/indesign/apsb20-66.html
CNVD-2020-57869	Mark Text 跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/marktext/marktext/issues/2360
CNVD-2020-57867	Anuko Time Tracker 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/anuko/timetracker/commit/d9472904361495f318c9d0294ffd28acaaeae42f
CNVD-2020-57866	Juniper Networks Junos OS 拒绝服务漏洞（CNVD-2020-57866）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11064

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用该漏洞实现任意代码执行。此外，Microsoft、Google、HPE 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取蓝牙服务器相关信息，实现本地权限提升，执行任意代码等。另外，GetSimpleCMS 产品被披露存在路径遍历漏洞。攻击者可利用该漏洞删除任意文件。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、MonoCMS Blog 信息泄露漏洞

验证描述

Mono 是一个由 Xamarin 公司（先前是 Novell，最早为 Ximian）所主持的自由开放源代码项目。

MonoCMS Blog 1.0 版本存在安全漏洞，该漏洞源于将硬编码的管理哈希存储在 MonoCMS Blog 的源文件中的 log.xml 文件中， 哈希类型是 bcrypt，哈希模式 3200 可用于破解哈希。

验证信息

POC 链接：https://packetstormsecurity.com/files/159430/MonoCMS-Blog-1.0-File-Deletion-CSRF-Hardcoded-Credentials.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-57872

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 为流行插件中的漏洞部署了强制安全更新

超过一百万的 WordPress 网站正在运行易受攻击的 Loginizer 插件版本。运行 Loginizer 插件的 WordPress 网站本周被强制更新为 Loginizer 版本 1.6.4。此版本包含针对危险的 SQL 注入漏洞的安全修复程序，该漏洞可能使黑客能够接管运行旧版 Loginizer 插件的 WordPress 网站。

参考链接：https://www.zdnet.com/article/wordpress-deploys-forced-security-update-for-dangerous-bug-in-popular-plugin/

2. VMware 修复了 ESXi，Workstation，Fusion 和 NSX-T 中的若干漏洞

VMware 修补了 ESXi，Workstation，Fusion 和 NSX-T 产品中的多个漏洞，包括一个关键的代码执行漏洞。跟踪为 CVE-2020-3992 的严重漏洞是一个先使用后使用的问题，它会影响 ESXi 中的 OpenSLP 服务。

参考链接：https://securityaffairs.co/wordpress/109843/security/vmware-critical-flaws.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