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 26 日-2020 年 11 月 01 日

2020 年第 44 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 418 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 5.79。本周收录的漏洞中，涉及 0day 漏洞 205 个（占 49%），其中互联网上出现“Nagios XI 'Contact Templates'跨站脚本漏洞、Small CRM 'email' SQL 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 9867 个，与上周（12085 个）环比减少 18%。

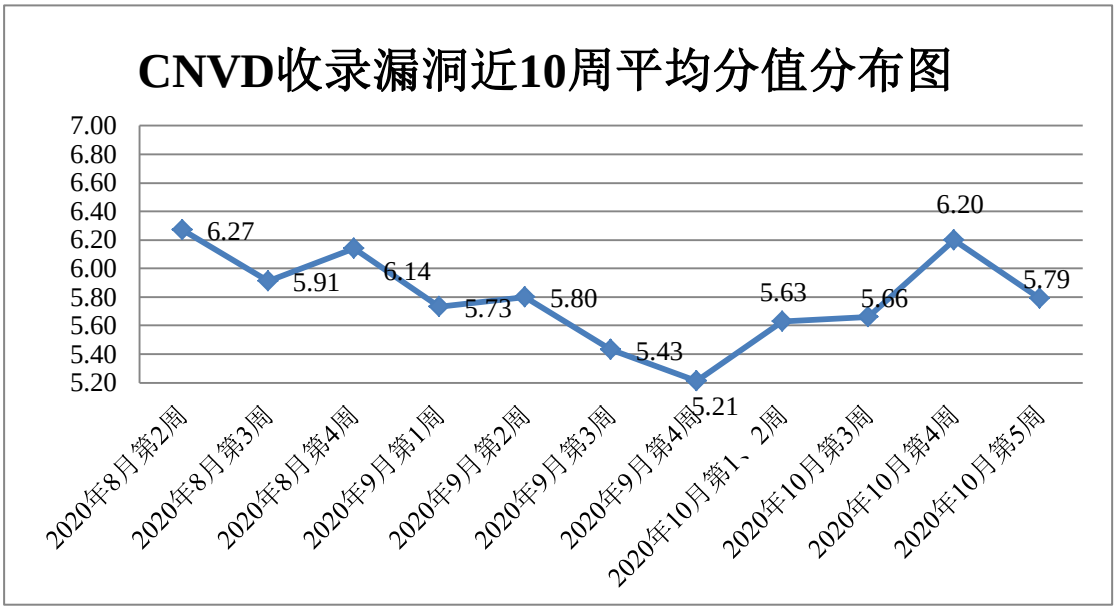

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 27 起，向基础电信企业通报漏洞事件 13 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 314 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 57 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 35 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：

青岛易企天创管理咨询有限公司、沈阳盘古网络技术有限公司、锐捷网络股份有限公司、上海牛迈网络科技有限公司、杭州巴零科技有限公司、北京引领盛世网络科技发展中心、西安紫云羚网络科技有限责任公司、酷溜网（北京）文化传媒有限公司、友讯电子设备（上海）有限公司、昆明云涛科技有限公司、北京六趣网络科技有限公司、浙江齐治科技股份有限公司、宁波网商信息科技有限公司、西安众邦网络科技有限公司、厦门帝易鑫软件科技有限公司、武汉贝云网络科技有限公司、西门子（中国）有限公司、广州网易计算机系统有限公司、天津速读科技有限公司、深圳市迅雷网文化有限公司、北京万维盈创科技发展有限公司、景腾多媒体股份有限公司、淄博闪灵网络科技有限公司、上海亿速网络科技有限公司、上海纵之格科技有限公司、深圳市乔安科技有限公司、欧姆龙自动化（中国）有限公司、上海金慧软件有限公司、成都飞鱼星科技股份有限公司、深圳银澎云计算有限公司、杭州瑞成信息技术有限公司、四创科技有限公司、华硕电脑（上海）有限公司、上海孚盟软件有限公司、北京珑大钜商科技有限公司、北京五指互联科技有限公司、湖南壹拾捌号网络技术有限公司、研华科技（中国）有限公司、北京百容千域软件技术开发有限责任公司、武汉创益云信息技术有限公司、北京国炬信息技术有限公司、深圳市星空量子科技有限公司、深圳市创实互联科技有限公司、上海泛微网络科技股份有限公司、青岛商至信网络科技有限公司、北京海腾时代科技有限公司、北京金考典教育科技有限公司、上海商派网络科技有限公司、北京力控元通科技有限公司、深圳华制智能制造技术有限公司、珠海金山办公软件有限公司、上海互盾信息科技有限公司、北京酷我科技有限公司、温州云通数达网络科技有限公司、完美世界（北京）软件科技发展有限公司、南京偲言睿网络科技有限公司、杭州凤侠网络科技有限公司、上海新浩艺软件有限公司、苏州开心盒子软件有限公司、武汉鲜牛网络科技有限公司、北京方正阿帕比技术有限公司、罗克韦尔自动化(中国)有限公司、重庆猫扑网络科技有限公司、北京通达信科科技有限公司、上海梵讯网络技术有限公司、台达集团、锦江区闪灵网络服务部、三菱电机、上海荃路软件开发工作室、智睿软件、狂雨小说 cms、梦想 CMS、ZZCMS、Hancom、Microsoft、ZrLog、ForestBlog、ShuipFCMS、TuziCMS、KuaiFanCMS、HRSALE、BEESCMS、Emlog、Yycms 和 CLTPHP。

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、北京神州绿盟科技有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、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。国瑞数码零点实验室、北京华云安信息技术有限公司、西安交大捷普网络科技有限公司、河南灵创电子科技有限公司、山东新潮信息技术有限公司、杭州迪普科技股份有限公司、河南信安世纪科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、上海观安信息技术股份有限公司、北京天地和兴科技有限公司、北京机沃科技有限公司、内蒙古奥创科技有限公司、南京众智维信息科技有限公司、浙江安腾信息技术有限公司、吉林谛听信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、安徽长泰信息安全服务有限公司、山石网科通信技术股份有限公司、山东道普测评技术有限公司、平安银河实验室、山东云天安全技术有限公司、京东云安全、四川哨兵信息科技有限公司、北京华顺信安科技有限公司、广州安亿信软件科技有限公司、北京零零信安科技有限公司、联想全球安全实验室、北京智游网安科技有限公司、中科信息安全共性技术国家工程研究中心有限公司、北京顶象技术有限公司、北京安全共识科技有限公司及其他个人白帽子向CNVD提交了9867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8780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
安信网神（补天平台）	7201	7201
斗象科技（漏洞盒子）	1170	1170
上海交大	409	409
北京天融信网络安全技术有限公司	312	5
北京神州绿盟科技有限公司	307	26
哈尔滨安天科技集团股份有限公司	211	0
华为技术有限公司	154	0
北京启明星辰信息安全技术有限公司	93	14
中国电信股份有限公司网络安全产品运营中心	90	0
新华三技术有限公司	78	0
深信服科技股份有限公司	73	0
中国电信集团系统集成有限责任公司	33	33

中新网络信息安全股份有限公司	23	23
沈阳东软系统集成工程有限公司	9	0
腾讯安全云鼎实验室	4	0
北京知道创宇信息技术股份有限公司	3	0
国家互联网应急中心	3	3
北京奇虎科技有限公司	1	1
国瑞数码零点实验室	139	139
北京华云安信息技术有限公司	50	50
西安交大捷普网络科技有限公司	29	29
河南灵创电子科技有限公司	23	23
山东新潮信息技术有限公司	22	22
杭州迪普科技股份有限公司	19	5
河南信安世纪科技有限公司	19	19
远江盛邦（北京）网络安全科技股份有限公司	10	10
上海观安信息技术股份有限公司	9	9
北京天地和兴科技有限公司	9	9
北京机沃科技有限公司	9	9
内蒙古奥创科技有限公司	8	8
南京众智维信息科技有限公司	8	8
浙江安腾信息技术有限公司	8	8
吉林谛听信息技术有限公司	6	6
北京云科安信科技有限公司（Seraph 安全实验室）	5	5

安徽长泰信息安全服务有限公司	5	5
山石网科通信技术股份有限公司	4	4
山东道普测评技术有限公司	4	4
平安银河实验室	3	3
山东云天安全技术有限公司	3	3
京东云安全	3	3
四川哨兵信息科技有限公司	3	3
北京华顺信安科技有限公司	2	2
广州安亿信软件科技有限公司	2	2
北京零零信安科技有限公司	2	2
联想全球安全实验室	1	1
北京智游网安科技有限公司	1	1
中科信息安全共性技术国家工程研究中心有限公司	1	1
北京顶象技术有限公司	1	1
北京安全共识科技有限公司	1	1
CNCERT 海南分中心	20	20
CNCERT 山西分中心	14	14
CNCERT 辽宁分中心	14	14
CNCERT 上海分中心	12	12
CNCERT 青海分中心	12	12
CNCERT 天津分中心	7	7
CNCERT 贵州分中心	6	6
CNCERT 浙江分中心	5	5

CNCERT 宁夏分中心	1	1
个人	496	496
报送总计	11170	9867

本周漏洞按类型和厂商统计

本周，CNVD 收录了 418 个漏洞。应用程序 215 个，WEB 应用 128 个，操作系统 16 个，数据库 25 个，网络设备（交换机、路由器等网络端设备）26 个，安全产品 5 个，智能设备（物联网终端设备）漏洞 3 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	215
WEB 应用	128
网络设备（交换机、路由器等网络端设备）	26
数据库	25
操作系统	16
安全产品	5
智能设备（物联网终端设备）	3

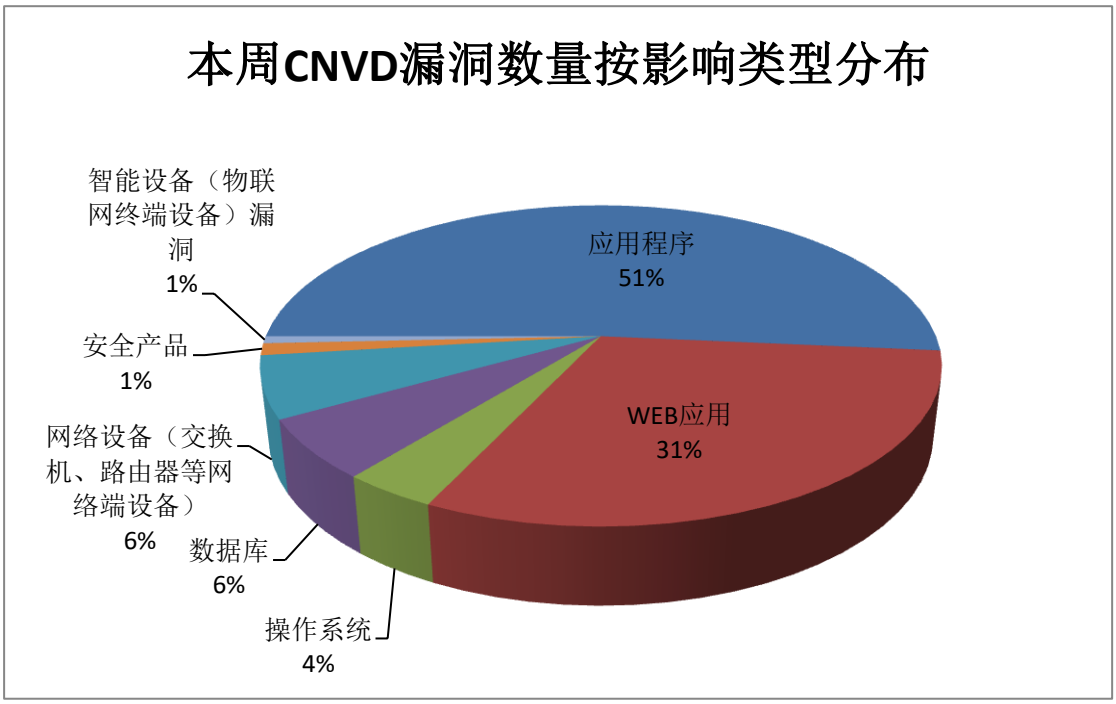

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、深圳市迅雷网文化有限公司、ZZCMS 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	51	12%
2	深圳市迅雷网文化有限公司	36	9%
3	ZZCMS	26	6%
4	Foxit	24	6%
5	IBM	20	5%
6	Apple	13	3%
7	HP	12	3%
8	CloudBees	9	2%
9	kkcms	7	2%
10	其他	220	52%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，16 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Google Android 资源管理错误漏洞（CNVD-2020-59732）、Apple iOS 任意代码执行漏洞（CNVD-2020-59479）”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/

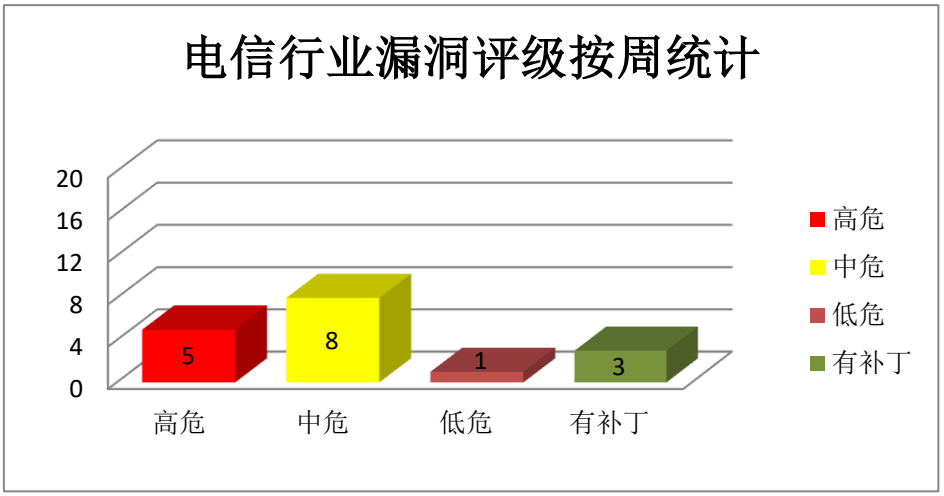

图 3 电信行业漏洞统计

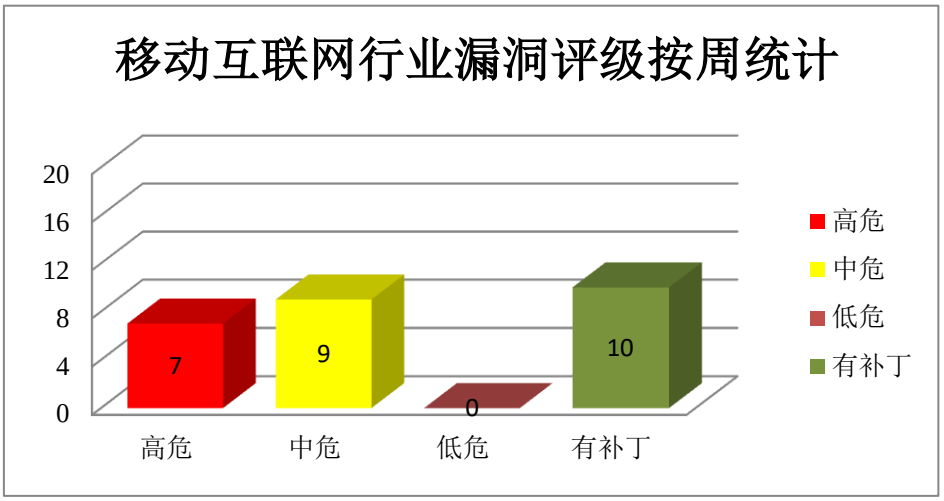

图 4 移动互联网行业漏洞统计

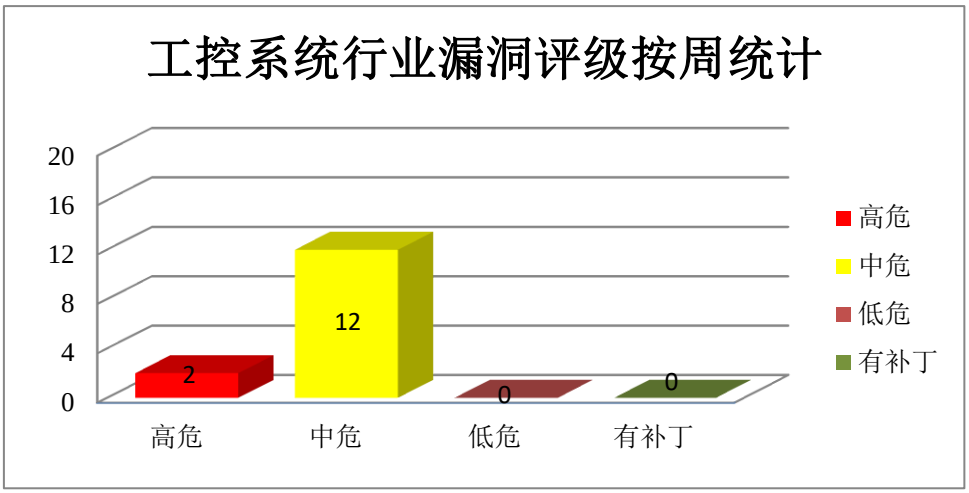

图 5 工控系统行业漏洞统计

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 macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple mac OS Catalina 是一套专为 Mac 计算机所开发的专用操作系统。Apple OS X 是一套为 Ma c 计算机所开发的专用操作系统。Apple iOS 是一套为移动设备所开发的操作系统。Ap ple tvOS 是一套智能电视操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。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，覆盖现有的文件，执行任意代码，导致意外的系统终止或损坏内核内存等。

CNVD 收录的相关漏洞包括：Apple macOS Mojave 未授权访问漏洞、Apple mac OS Catalina 任意文件覆盖漏洞、Apple macOS Catalina Bluetooth 内存破坏漏洞、Appl e macOS Catalina 缓冲区溢出漏洞、Apple 多款产品输入验证漏洞、Apple iOS 任意代

码执行漏洞（CNVD-2020-59479）、多款 Apple 产品缓冲区溢出漏洞（CNVD-2020-59731）、Apple macOS Catalina Kernel 信息泄露漏洞。其中，“Apple macOS Catalina 缓冲区溢出漏洞、Apple 多款产品输入验证漏洞、Apple iOS 任意代码执行漏洞（CNVD-2020-59479）”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-2020-59471
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59470
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59475
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59476
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59477
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59479
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59731
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59753

2、IBM 产品安全漏洞

IBM Oracle REST Data Services（ORDS）是一个 JAVA Web 的中间件应用。IBM QRadar SIEM 是一套利用安全智能保护资产和信息远离高级威胁的解决方案。IBM Cúram Social Program Management（SPM）是一套社会计划管理解决方案。IBM Security Access Manager 是一款应用于信息安全管理的产品。IBM WebSphere Application Server（WAS）是一款应用服务器产品。IBM Sterling Connect：Direct 是一套基于文件的点对点文件传输解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，获取敏感信息，执行客户端代码，导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：IBM Oracle REST Data Services 信息泄露漏洞、IBM Oracle REST Data Services 未授权访问漏洞、IBM QRadar SIEM 欺骗漏洞、IBM Cúram Social Program Management 访问控制错误漏洞、IBM Security Access Manager 安全绕过漏洞（CNVD-2020-59030）、IBM Cúram Social Program Management 跨站脚本漏洞（CNVD-2020-59038）、IBM WebSphere Application Server 路径遍历漏洞（CNVD-2020-59728）、IBM Sterling Connect:Direct Windows 缓冲区溢出漏洞。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-2020-58766
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58770
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58780
https://www.cnvd.org.cn/flaw/show/CNVD-2020-58779
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59030
https://www.cnvd.org.cn/flaw/show/CNVD-2020-59038

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59728

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59729

3、HPE 产品安全漏洞

HPE Intelligent Management Center 是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) sshconfig 表达式语言注入远程代码执行漏洞（CNVD-2020-58754）、HPE Intelligent Management Center (iMC) smsrulesdownload 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) forwardredirect 表达式语言注入远程代码执行漏洞（CNVD-2020-58755）、HPE Intelligent Management Center (iMC) faultflasheventselectfact 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) reportpage 索引表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) powershellconfigcontent 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) devsoftsel 表达式语言注入远程代码执行漏洞、HPE Intelligent Management Center (iMC) deviceselect 表达式语言注入远程代码执行漏洞（CNVD-2020-58762）。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-2020-58754

https://www.cnvd.org.cn/flaw/show/CNVD-2020-58753

https://www.cnvd.org.cn/flaw/show/CNVD-2020-58755

https://www.cnvd.org.cn/flaw/show/CNVD-2020-58761

https://www.cnvd.org.cn/flaw/show/CNVD-2020-58759

https://www.cnvd.org.cn/flaw/show/CNVD-2020-58758

https://www.cnvd.org.cn/flaw/show/CNVD-2020-58763

https://www.cnvd.org.cn/flaw/show/CNVD-2020-58762

4、Foxit 产品安全漏洞

Foxit Studio Photo 是一套图像编辑软件。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Foxit Studio Photo 远程代码执行漏洞（CNVD-2020-59766、CNVD-2020-59774、CNVD-2020-59775、CNVD-2020-59780、CNVD-2020-59779、CNVD-2020-59778、CNVD-2020-59782、CNVD-2020-59781）。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-2020-59766

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59774

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59775

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59780

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59779

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59778

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59782

https://www.cnvd.org.cn/flaw/show/CNVD-2020-59781

5、Belkin LINKSYS WRT160NL 缓冲区溢出漏洞

Belkin LINKSYS WRT160NL 是一款无线路由器。本周，Belkin LINKSYS WRT160NL 产品被披露存在缓冲区溢出漏洞。该漏洞源于 sprintf 在 mini_httpd create_dir，攻击者可利用该漏洞会导致任意的代码执行。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-2020-59744

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-2020-58773	JetBrains YouTrack 服务器端请求伪造漏洞（CNVD-2020-58773）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://blog.jetbrains.com/blog/2020/08/06/jetbrains-security-bulletin-q2-2020/
CNVD-2020-58775	Zoho ManageEngine Desktop Central 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.manageengine.com/products/desktop-central/integer-overflow-vulnerability.html
CNVD-2020-59042	Pexip Infinity 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://docs.pexip.com/admin/security_bulletins.htm
CNVD-2020-59212	Aruba Airwave Software 远程命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbnw04051en_us
CNVD-2020-59209	Aruba Airwave Software 未授权访问漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-hpesbnw04051en_us

CNVD-2020-59718	Gophish CSV 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/gophish/gophish/releases/tag/v0.11.0
CNVD-2020-59740	Aruba Airwave Software 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.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-hpesbnw04051en_us
CNVD-2020-59747	Cisco Firepower 2100 系列拒绝服务漏洞	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-ftd-ssl-dcrpt-dos-RYEkX4yy
CNVD-2020-59750	Microsoft Windows Office 代码注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-oct
CNVD-2020-59762	Hashicorp Vault AWS IAM Integration 认证绕过漏洞	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.hashicorp.com/blog/category/vault/

小结：本周，Apple 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，覆盖现有的文件，执行任意代码，导致意外的系统终止或损坏内核内存等。此外，IBM、HPE、Foxit 等多款产品被披露存在多个漏洞，攻击者可利用漏洞进行欺骗攻击，获取敏感信息，执行代码，导致应用程序崩溃等。另外，Belkin LINKSYS WRT160NL 产品被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞会导致任意的代码执行。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、Nagios XI 'Contact Templates'跨站脚本漏洞

验证描述

Nagios XI 是一套 IT 基础设施监控解决方案。该方案支持对应用、服务、操作系统等进行监控和预警。

Nagios XI 'Contact Templates'跨站脚本漏洞。攻击者可利用漏洞在受影响站点的上下文中执行任意脚本代码，允许攻击者窃取基于 cookie 的身份验证凭据并发起其他攻击。

验证信息

POC 链接：https://www.exploit-db.com/exploits/48893

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-59759

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. Nitro PDF 数据泄露可能会影响微软、谷歌和苹果

Nitro PDF 遭受的大规模数据泄露可能会对包括 Google，Apple，Microsoft，Chase 和 Citibank 在内的知名组织产生严重影响。该公司在全球拥有超过 650,000 个商业客户，并在全球拥有数百万用户。

参考链接：https://securityaffairs.co/wordpress/110025/data-breach/nitro-pdf-data-breach.html

2. 承诺会保护隐私的社交应用 True 却意外曝光用户私人数据

True 自称是一款能够“保护你的隐私”的社交网络应用。但由于安全漏洞，该公司的一台服务器却曝光了用户私人数据。这款应用于 2017 年由 Hello Mobile 推出，Hello Mobile 是一家虚拟手机运营商，依附于 T-Mobile 的网络。

参考链接：https://www.cnbeta.com/articles/tech/1046645.htm

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