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 08 日-2020 年 06 月 14 日　　2020 年第 24 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 563 个，其中高危漏洞 211 个、中危漏洞 294 个、低危漏洞 58 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 239 个（占 42%），其中互联网上出现“Subrion CMS 跨站请求伪造漏洞（CNVD-2020-32357）、Subrion CMS 跨站脚本漏洞（CNVD-2020-32356）”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 2100 个，与上周（3065 个）环比减少 31%。

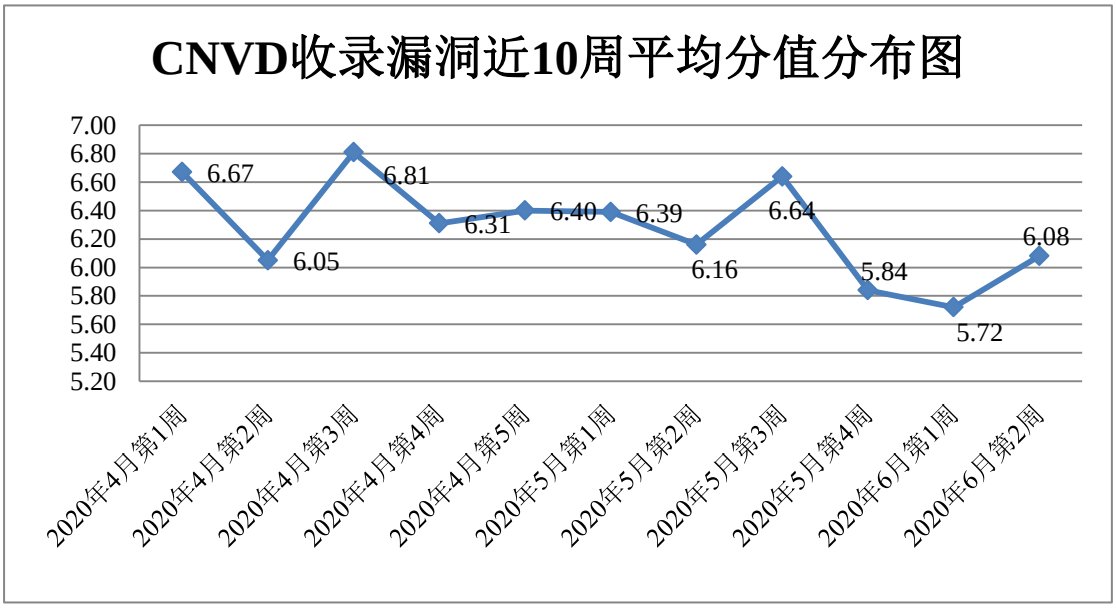

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向基础电信企业通报漏洞事件 10 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 211 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 50 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 23 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：

合肥奇乐网络科技有限公司、东莞市光速网络技术有限公司、沈阳盘古网络技术有限公司、洪湖尔创网联信息技术有限公司、河南跃龙门科技有限公司、金华市亿途网络科技有限公司、用友网络科技股份有限公司、宿迁鑫潮信息技术限公司、珠海金山办公软件有限公司、济南卓源软件有限公司、哈尔滨伟成科技有限公司、青岛商至信网络科技有限公司、深圳市锟铻科技有限公司、北京中金云创软件有限公司、宿迁市展鸿网络科技有限公司、茉柏枘（上海）软件科技有限公司、寻乌云橙信息科技有限公司、上海卓岚信息科技有限公司、廊坊市极致网络科技有限公司、山西企凝信息科技有限公司、杭州益仕行信息技术有限公司、南京先极科技有限公司、酷溜网（北京）文化传媒有限公司、南京怀宇科技有限公司、北京智量科技有限公司、石家庄酷艺网络科技有限公司、龙采科技（山西）有限公司、北京百容千域软件技术开发有限责任公司、成都爱诚科技有限公司、湖北淘码千维信息科技有限公司、北京亚控科技发展有限公司、大唐软件技术股份有限公司、浪潮软件集团有限公司、南充市老虎云网络技术有限公司、景腾多媒体股份有限公司、江下信息科技（惠州）有限公司、北京泛在时代教育技术有限责任公司、江苏易索电子科技股份有限公司、宁波易则力网络科技有限公司、石家庄百成网络科技有限公司、上海海典软件股份有限公司、澳通（大连）科技发展有限公司、深圳市乙辰科技股份有限公司、酷溜网（北京）科技有限公司、深圳市驱动人生科技股份有限公司、六安校无忧信息科技有限公司、广西金中软件有限公司、索尼（中国）有限公司、海南赞赞网络科技有限公司、广东顺德德韵网络科技有限公司、长沙米拓信息技术有限公司、南通云尚找家纺电子商务有限公司、陕西金推信息技术有限公司、镇江市云优网络科技有限公司、江苏图星软件科技有限责任公司、邮箱宿迁市展鸿网络科技有限公司、淄博闪灵网络科技有限公司、北京为因软件、无忧网络、上海荃路软件开发工作室、中国残疾人联合会、信呼、正光网络、袁志蒙工作室、山石网科、DM 企业建站系统、Blog-System、115CMS、Uublog、PHPEMS、Zzzcms、BEESCMS、Jflyfox、My-Blog-layui、ZZCMS、Guojiz 和 TVHeadend。

本周，CNVD 发布了《Microsoft 发布 2020 年 6 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5567

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，恒安嘉新(北京)科技股份公司、华为技术有限公

司、哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、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。北京华云安信息技术有限公司、山东道普测评技术有限公司、河南灵创电子科技有限公司、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、杭州迪普科技股份有限公司、国瑞数码零点实验室、吉林谛听信息技术有限公司、山东云天安全技术有限公司、河北华测信息技术有限公司、北京天地和兴科技有限公司、京东云安全、内蒙古洞明科技有限公司、四川哨兵信息科技有限公司、国家互联网应急中心、河南信安世纪科技有限公司、上海观安信息技术股份有限公司、上海上讯信息技术股份有限公司、北京顶象技术有限公司、中国—东盟信息港股份有限公司、北京智游网安科技有限公司、南瑞集团公司（国网电力科学研究院）、南方电网数字电网研究院有限公司、上海纽盾科技股份有限公司、国网山东省电力公司及其他个人白帽子向 CNVD 提交了 2100 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 1470 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）	917	917
恒安嘉新(北京)科技股份公司	370	0
奇安信网神（补天平台）	292	292
上海交大	261	261
华为技术有限公司	244	0
哈尔滨安天科技集团股份有限公司	214	0
北京天融信网络安全技术有限公司	141	20
新华三技术有限公司	95	0
深信服科技股份有限公司	88	0
厦门服云信息科技有限公司	84	0
北京启明星辰信息安全技术有限公司	79	1
北京神州绿盟科技有限公司	69	27

北京奇虎科技有限公司	58	14
北京数字观星科技有限公司	30	0
沈阳东软系统集成工程有限公司	4	4
北京知道创宇信息技术股份有限公司	2	1
深圳市腾讯计算机系统有限公司（玄武实验室）	2	1
北京华云安信息技术有限公司	100	100
山东道普测评技术有限公司	41	41
河南灵创电子科技有限公司	23	23
远江盛邦（北京）网络安全科技股份有限公司	21	21
长春嘉诚信息技术股份有限公司	19	19
杭州迪普科技股份有限公司	14	0
国瑞数码零点实验室	13	13
吉林谛听信息技术有限公司	7	7
山东云天安全技术有限公司	6	6
河北华测信息技术有限公司	5	5
北京天地和兴科技有限公司	5	5
京东云安全	3	3
内蒙古洞明科技有限公司	2	2
四川哨兵信息科技有限公司	2	2
国家互联网应急中心	2	2
河南信安世纪科技有限公司	1	1
上海观安信息技术股份有限公司	1	1

上海上讯信息技术股份有限公司	1	1
北京顶象技术有限公司	1	1
中国—东盟信息港股份有限公司	1	1
北京智游网安科技有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
南方电网数字电网研究院有限公司	1	1
上海纽盾科技股份有限公司	1	1
国网山东省电力公司	1	1
CNCERT 西藏分中心	6	6
CNCERT 四川分中心	3	3
CNCERT 山西分中心	2	2
CNCERT 青海分中心	1	1
个人	291	291
报送总计	3526	2100

本周漏洞按类型和厂商统计

本周，CNVD 收录了 563 个漏洞。应用程序 234 个，WEB 应用 186 个，操作系统 123 个，网络设备（交换机、路由器等网络端设备）14 个，智能设备（物联网终端设备）4 个，安全产品 2 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	234
WEB 应用	186
操作系统	123
网络设备（交换机、路由器等网络端设备）	14
智能设备（物联网终端设备）漏洞	4
安全产品	2

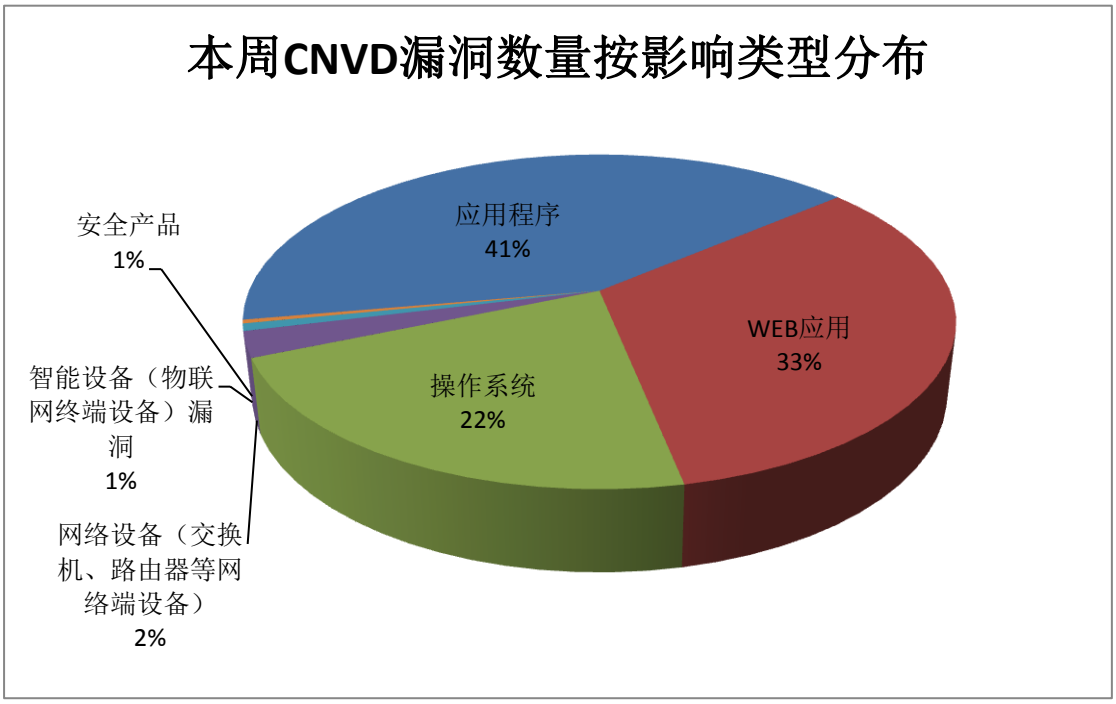

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Foxit、Cisco 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	79	14%
2	Foxit	47	8%
3	Cisco	38	7%
4	Adobe	37	7%
5	Microsoft	26	5%
6	延边州石头网络科技服务中心	26	5%
7	IBM	21	4%
8	Palo Alto Networks	12	2%
9	珠海金山办公软件有限公司	8	1%
10	其他	269	47%

本周行业漏洞收录情况

本周，CNVD 收录了 21 个电信行业漏洞，79 个移动互联网行业漏洞，19 个工控行业漏洞（如下图所示）。其中，“IBM WebSphere Application Server 代码问题漏洞（CN

VD-2020-32642）、Cisco IOS XE 命令注入漏洞（CNVD-2020-31974）、Apple macOS Catalina Wi-Fi 组件内存破坏漏洞（CNVD-2020-32218）、Advantech WebAccess Node 缓冲区溢出漏洞（CNVD-2020-32232）、Emerson OpenEnterprise 关键功能认证缺失漏洞”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/

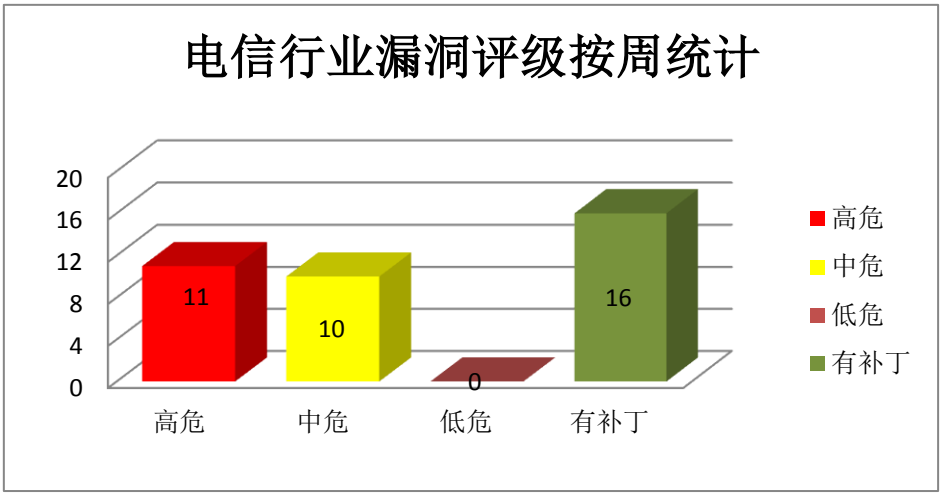

图 3 电信行业漏洞统计

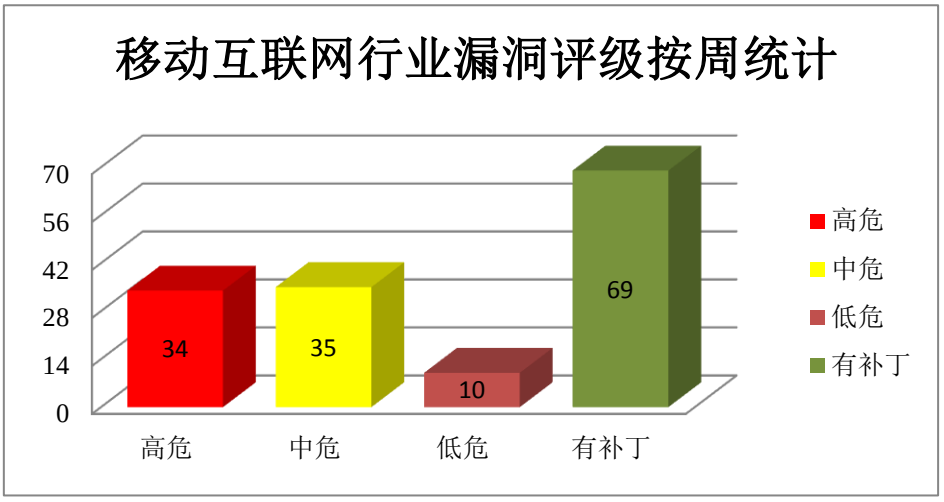

图 4 移动互联网行业漏洞统计

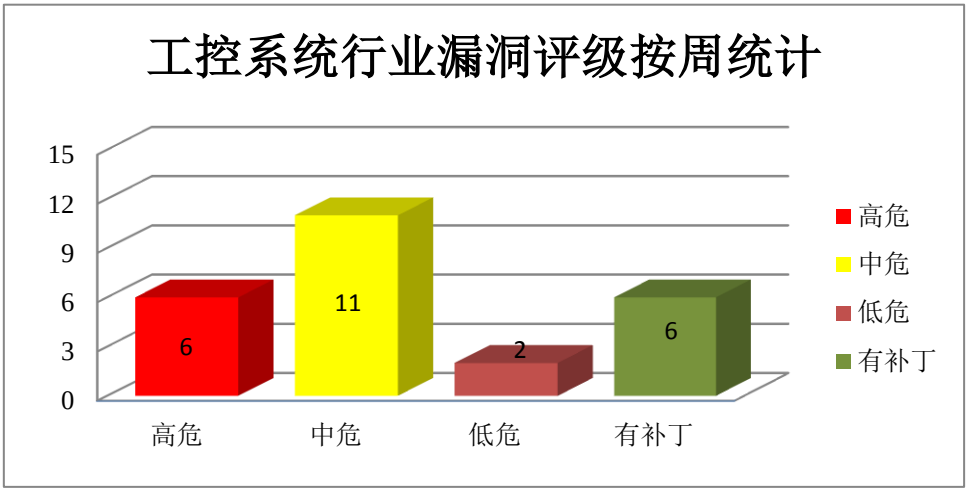

图 5 工控系统行业漏洞统计

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、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。Microsoft SharePoint 是一套企业业务协作平台。Microsoft Teams 是一个流行的协同交互应用。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，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 提权漏洞（CNVD-2020-32093）、Microsoft SharePoint 跨站脚本漏洞（CNVD-2020-32097）、Microsoft Windows Jet Database Engine 远程代码执行漏洞（CNVD-2020-32587）、Microsoft Windows Push Notification Service 权限提升漏洞、Microsoft Windows win32k 权限提升漏洞（CNVD-2020-32590、CNVD-2020-32589、CNVD-2020-32588）、Microsoft Teams 用户劫持漏洞。其中，除“Microsoft SharePoint 跨站脚本漏洞（CNVD-2020-32097）”外，其余漏洞的综合评级为“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-2020-32093

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32097

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32587

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32584

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32590

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32589

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32588

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32725

2、Adobe 产品安全漏洞

Adobe Bridge 是一款文件查看器。Adobe Flash Player 是一种广泛使用的、专有的多媒体程序播放器。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Reader 是一套 PDF 文档阅读软件。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，导致拒绝服务。

CNVD 收录的相关漏洞包括：Adobe Bridge 代码执行漏洞（CNVD-2020-32370、CNVD-2020-32371）、Adobe Flash Player 内存错误引用漏洞（CNVD-2020-32617）、Adobe Acrobat 和 Reader 内存错误引用漏洞（CNVD-2020-32834、CNVD-2020-32836）、Adobe Acrobat 和 Reader 缓冲区溢出漏洞（CNVD-2020-32837、CNVD-2020-32838）、Adobe Acrobat 和 Reader 栈耗尽漏洞。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-2020-32371

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32370

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32617

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32834

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32837

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32836

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32838

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32846

3、Cisco 产品安全漏洞

Cisco IOS XE 是一套为其网络设备开发的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco IOS XE 命令注入漏洞（CNVD-2020-31959、CNVD-2020-31962、CNVD-2020-31969、CNVD-2020-31974）、Cisco IOS XE 权限许可和访问控制问题漏洞（CNVD-2020-31964、CNVD-2020-31976）、Cisco IOS XE Software 输入验证错误漏洞、Cisco IOS XE 数据伪造问题漏洞（CNVD-2020-31991）。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-2020-31959

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31962

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31964

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31970

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31969

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31974

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31976

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31991

4、IBM 产品安全漏洞

IBM MobileFirst Foundation 是一套用于构建和部署下一代数字应用程序的平台。IBM WebSphere Application Server（WAS）是一款应用服务器产品。IBM Security Guardium 是一套提供数据保护功能的平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未授权访问会话，获取敏感信息，执行任意命令等。

CNVD 收录的相关漏洞包括：IBM MobileFirst Foundation 授权问题漏洞、IBM WebSphere Application Server 代码问题漏洞（CNVD-2020-32642）、IBM WebSphere Application Server Network Deployment 代码问题漏洞、IBM Security Guardium 信息泄露漏洞（CNVD-2020-32645、CNVD-2020-32650）、IBM Security Guardium 操作系统命令注入漏洞（CNVD-2020-32648）、IBM Security Guardium 跨站脚本漏洞（CNVD-2020-32644、CNVD-2020-32649）。其中，“IBM MobileFirst Foundation 授权问题漏洞、IBM WebSphere Application Server 代码问题漏洞（CNVD-2020-32642）、IBM WebSphere Application Server Network Deployment 代码问题漏洞、IBM Security Guardium 操作系统命令注入漏洞（CNVD-2020-32648）”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-2020-32639

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32642

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32640

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32645

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32644

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32648

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32650

https://www.cnvd.org.cn/flaw/show/CNVD-2020-32649

5、Red Hat Undertow 输入验证错误漏洞

Red Hat Undertow 是美国红帽（Red Hat）公司的一款基于 Java 的嵌入式 Web 服务器。本周，Red Hat Undertow 被披露存在输入验证错误漏洞。攻击者可利用该漏洞造成 Web 缓存中毒，执行跨站脚本攻击或获取敏感信息。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-2020-32367

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-2020-32217	Apple macOS Catalina Wi-Fi 组件内存破坏漏洞（CNVD-2020-32217）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/zh-cn/HT211170
CNVD-2020-32232	Advantech WebAccess Node 缓冲区溢出漏洞（CNVD-2020-32232）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.advantech.com/support/DownloadSRDetail_New.aspx?SR_ID=1-MS9MJV&Doc_Source=Download
CNVD-2020-32235	Palo Alto Networks PAN-OS 任意文件删除漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.paloaltonetworks.com/CVE-2020-2003
CNVD-2020-32363	FreeBSD ipfw 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://security.freebsd.org/advisories/FreeBSD-SA-20:10.ipfw.asc
CNVD-2020-32425	Ivanti Avalanche SQL 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://forums.ivanti.com/s/article/SQL-Injection-Vulnerability-in-Avalanche
CNVD-2020-32434	Fortinet FortiMail 和 FortiVoice Entreprise 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://fortiguard.com/psirt/FG-IR-20-045
CNVD-2020-32664	Emerson OpenEnterprise 关键功能认证缺失漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.us-cert.gov/ics/advisories/icsa-20-140-02
CNVD-2020-32791	Samsung 移动设备代码执行漏洞（CNVD-2020-32791）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.samsungmobile.com/securityUpdate.smsb
CNVD-2020-32851	Dell EMC Integrated Data Protection Appliance 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.dell.com/support/security/en-us/details/542518/DSA-2020-079-Dell-EMC-Integrated-Data-Protection-Appliance-Command-Injection-Vulnerability
CNVD-2020-	Apache IoTDB 信任管理问题	高	目前厂商已发布升级补丁以修复漏

32886	漏洞		洞，补丁获取链接：https://lists.apache.org/thread.html/r3d2ff899ead64d2952fdc1fbb1f520ca42011ed2b4c7f786e921f6b9%40%3Cdev.iotdb.apache.org%3E

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，获取敏感信息，执行任意代码等。此外 Adobe、Cisco、IBM 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，获取敏感信息，执行任意代码，导致拒绝服务等。另外，Red Hat Undertow 被披露存在输入验证错误漏洞。攻击者可利用该漏洞造成 Web 缓存中毒，执行跨站脚本攻击或获取敏感信息。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、Subrion CMS 跨站脚本漏洞（CNVD-2020-32356）

验证描述

Subrion CMS 是 Subrion 团队的一套基于 PHP 的内容管理系统（CMS）。该系统可被集成到网站，并支持多种扩展插件等。

Subrion CMS 4.2.1 版本中的/panel/configuration/general 设置页面存在跨站脚本漏洞，远程攻击者可借助‘v[language_switch]’参数利用该漏洞注入任意的 JavaScript 代码。

验证信息

POC 链接：https://packetstormsecurity.com/files/157699/Subrion-CMS-4.2.1-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-32356

信息提供者

恒安嘉新(北京)科技股份公司

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. D-Link 发布了一个新的安全固件

D-Link 最近发布了固件更新，但该更新仅能修复 DIR-865L 家用无线路由器六个安

全漏洞中的三个。

参考链接：https://securityaffairs.co/wordpress/104684/security/d-link-dir-865l-flaws.html

2. 英特尔处理器又曝两个 SGX 新漏洞，攻击者可轻松提取敏感数据

当英特尔努力消除多个处理器漏洞造成的负面影响的时候，三所大学的安全研究人员再次无情地曝光了 SGX 软件防护扩展指令的另外两个漏洞。对于攻击者来说，这可以让他们相当轻松地提取敏感数据。

参考链接：https://www.cnbeta.com/articles/tech/989711.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