国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 03 月 23 日-2020 年 03 月 29 日　　2020 年第 13 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 504 个，其中高危漏洞 215 个、中危漏洞 242 个、低危漏洞 47 个。漏洞平均分值为 6.36。本周收录的漏洞中，涉及 0day 漏洞 188 个（占 37%），其中互联网上出现“YzmCMS 'url'跨站脚本漏洞、Sumavision Enhanced Multimedia Router 跨站请求伪造漏洞”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 3354 个，与上周（2662 个）环比增加 26%。

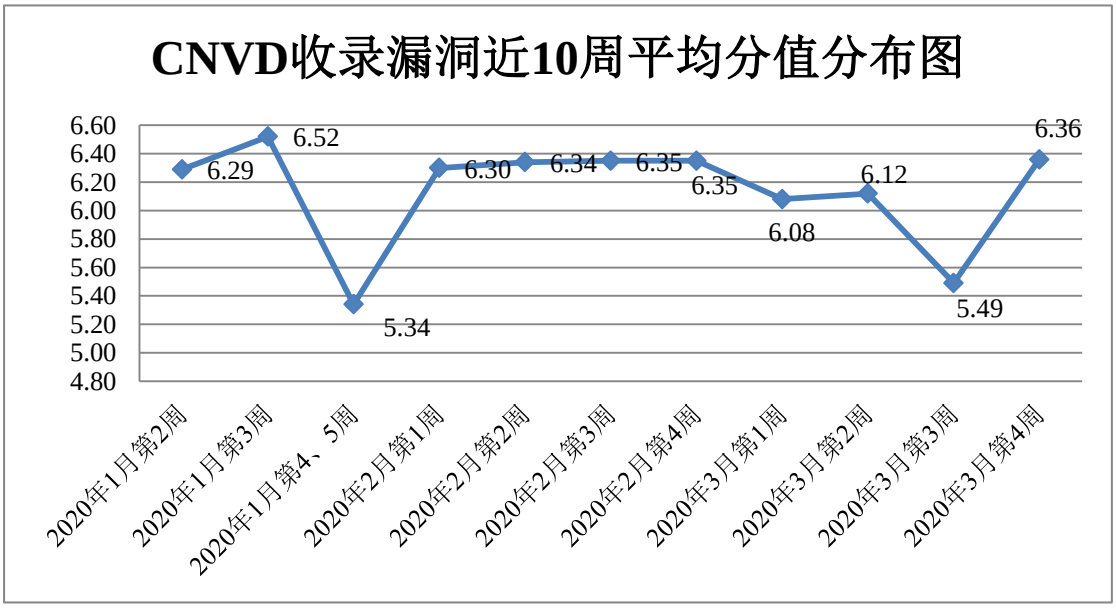

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 13 起，向基础电信企业通报漏洞事件 8 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 387 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 34 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 8 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：

潮州市微派网络科技有限公司、湖北淘码千维信息科技有限公司、北京良精志诚科技有限责任公司、通用电气（GE）公司、深圳市福洽科技有限公司、杭州启博科技有限公司、极致网络科技有限公司、青岛商至信网络科技有限公司、上海茸易科技有限公司、广州爱搜客网络科技有限公司、中国惠普有限公司、四川艾普视达数码科技有限公司、南充市老虎云网络技术有限公司、青岛网搜网络技术有限公司、合肥几度互联网络科技有限公司、灵宝简好网络科技有限公司、湖南心艾网络科技有限公司、深圳市科图自动化新技术应用公司、北京勤云科技发展有限公司、福州网钛软件科技有限公司、山东渔翁信息技术股份有限公司、杭州卷瓜网络有限公司、北京联高软件开发有限公司、上海企炬广告传媒有限公司、台安科技（无锡）有限公司、北京腾控科技有限公司、镇江市云优网络科技有限公司、广州购啊购科技有限公司、星网锐捷网络技术有限公司、正方软件股份有限公司、厦门海为科技有限公司、福建福昕软件开发股份有限公司、上海丹帆网络科技有限公司、施耐德电气有限公司、北京通达信科科技有限公司、广州思迈特软件有限公司、上海泛微网络科技股份有限公司、湖南翱云网络科技有限公司、苏州科达科技股份有限公司、天闻数媒科技有限公司、昆明云涛科技有限公司、广州荔支网络技术有限公司、武汉贝云网络科技有限公司、山西企凝信息科技有限公司、深圳市锟铻科技有限公司、淄博闪灵网络科技有限公司、北京创讯未来软件技术有限公司、北京至诚悠远科技有限公司、廊坊市极致网络科技有限公司、安徽易商数码科技有限公司、合肥一浪网络科技有限公司、北京五指互联科技有限公司、北京世纪超星信息技术发展有限责任公司、海南创想未来文化传媒有限公司、黑龙江资海科技集团股份有限公司、北京智量科技有限公司、苏州宇腾网络信息技术服务有限公司、名炬企业管理（上海）有限公司、ABB 集团、网展科技、华科网络、信呼、鹏博士集团长城宽带、乐尚商城开源系统、乘风原创程序、易贝 CMS、LOGA 建站系统、华夏 ERP、zzz 中文网、Heybbs、Allen-Bradley、Guojiz、DNSTracer、ShowDoc、MyuCMS、YUZHIGUO CMS、uqcms、YCCMS、115CMS、SeaCMS、CatfishCMS、UWA 和大米 CMS。

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、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、华为技术有限公司、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。北京华云安信息技术有限公司、南京众智维信息科技有限公司、内蒙古奥创科技有限公司、杭州迪普科技股份有限公司、

长春嘉诚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、河南灵创电子科技有限公司、山东新潮信息技术有限公司、北京圣博润高新技术股份有限公司、上海观安信息技术股份有限公司、北京铭图天成信息技术有限公司、国瑞数码零点实验室、北京机沃科技有限公司、北京信联科汇科技有限公司、东莞市百塔网络科技有限公司、山石网科通信技术股份有限公司、河北千诚电子科技有限公司、广西网信信息安全等级保护测评有限公司、河南信安世纪科技有限公司、深圳市魔方安全科技有限公司、北京智游网安科技有限公司、安吉加加信息技术有限公司、广州万方计算机科技有限公司、南瑞集团公司（国网电力科学研究院）、厦门靠谱云股份有限公司、山东云天安全技术有限公司及其他个人白帽子向 CNVD 提交了 3354 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 2172 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）	929	929
奇安信网神（补天平台）	679	679
上海交大	564	564
恒安嘉新(北京)科技股份公司	339	0
北京天融信网络安全技术有限公司	257	7
哈尔滨安天科技集团股份有限公司	242	0
华为技术有限公司	131	0
深信服科技股份有限公司	89	0
北京启明星辰信息安全技术有限公司	75	0
中新网络信息安全股份有限公司	72	72
新华三技术有限公司	66	0
中国电信集团系统集成有限责任公司	60	60
北京数字观星科技有限公司	29	0
北京神州绿盟科技有限公司	25	0

北京奇虎科技有限公司	25	0
西安四叶草信息技术有限公司	25	25
杭州安恒信息技术股份有限公司	16	16
四川无声信息技术有限公司	13	13
南京联成科技发展股份有限公司	11	11
北京知道创宇信息技术股份有限公司	3	0
北京安信天行科技有限公司	2	2
南京铱迅信息技术股份有限公司	1	1
北京华云安信息技术有限公司	147	147
南京众智维信息科技有限公司	113	113
内蒙古奥创科技有限公司	64	64
杭州迪普科技股份有限公司	64	0
长春嘉诚信息技术股份有限公司	55	55
远江盛邦（北京）网络安全科技股份有限公司	39	39
河南灵创电子科技有限公司	35	35
山东新潮信息技术有限公司	32	32
北京圣博润高新技术股份有限公司	17	17
上海观安信息技术股份有限公司	13	13
北京铭图天成信息技术有限公司	9	9
国瑞数码零点实验室	9	9
北京机沃科技有限公司	7	7
北京信联科汇科技有限公司	4	4

东莞市百塔网络科技有限公司	3	3
山石网科通信技术股份有限公司	3	3
河北千诚电子科技有限公司	2	2
广西网信信息安全等级保护测评有限公司	2	2
河南信安世纪科技有限公司	2	2
深圳市魔方安全科技有限公司	2	2
北京智游网安科技有限公司	1	1
安吉加加信息技术有限公司	1	1
广州万方计算机科技有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
厦门靠谱云股份有限公司	1	1
山东云天安全技术有限公司	1	1
CNCERT 海南分中心	7	7
CNCERT 吉林分中心	3	3
CNCERT 河南分中心	2	2
CNCERT 福建分中心	1	1
CNCERT 广西分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 四川分中心	1	1
CNCERT 天津分中心	1	1
个人	394	394
报送总计	4692	3354

本周漏洞按类型和厂商统计

本周，CNVD 收录了 504 个漏洞。应用程序 230 个，WEB 应用 153 个，网络设备（交换机、路由器等网络端设备）55 个，操作系统 37 个，安全产品 26 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	230
WEB 应用	153
网络设备（交换机、路由器等网络端设备）	55
操作系统	37
安全产品	26
智能设备（物联网终端设备）	3

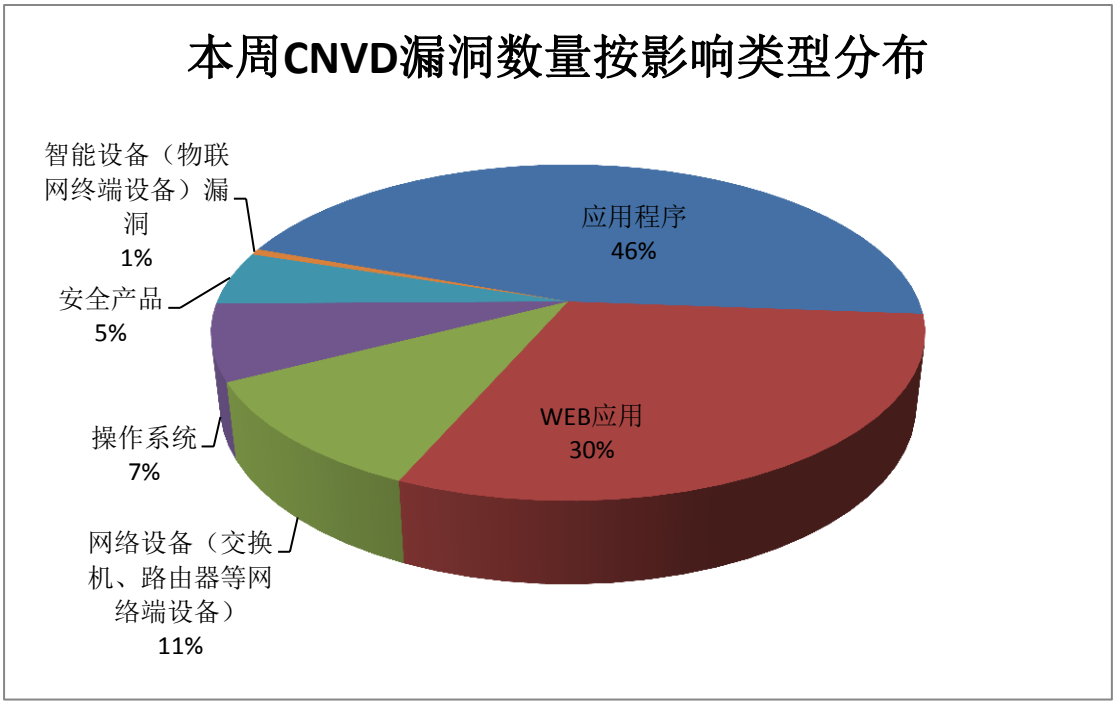

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、GitLab、深圳市迪元素科技有限公司等多家厂商的产品，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	Microsoft	28	6%
2	GitLab	23	5%
3	深圳市迪元素科技有限公司	21	4%

4	IBM	18	4%
5	Intel	14	2%
6	Cisco	10	2%
7	Google	10	2%
8	SemCms	10	2%
9	Chadha Software Technologies	9	2%
10	其他	361	71%

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，10 个移动互联网行业漏洞，26 个工控行业漏洞（如下图所示）。其中，“Siemens SIMATIC S7-300 CPU and SINUMERIK Controller 资源管理错误漏洞、Advantech WebAccess 缓冲区溢出漏洞（CNVD-2020-19926）、TP-Link Archer A7 AC1750 操作系统命令注入漏洞、Google Android 代码执行漏洞（CNVD-2020-19577）、TP-Link Archer A7 AC1750 缓冲区溢出漏洞”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/

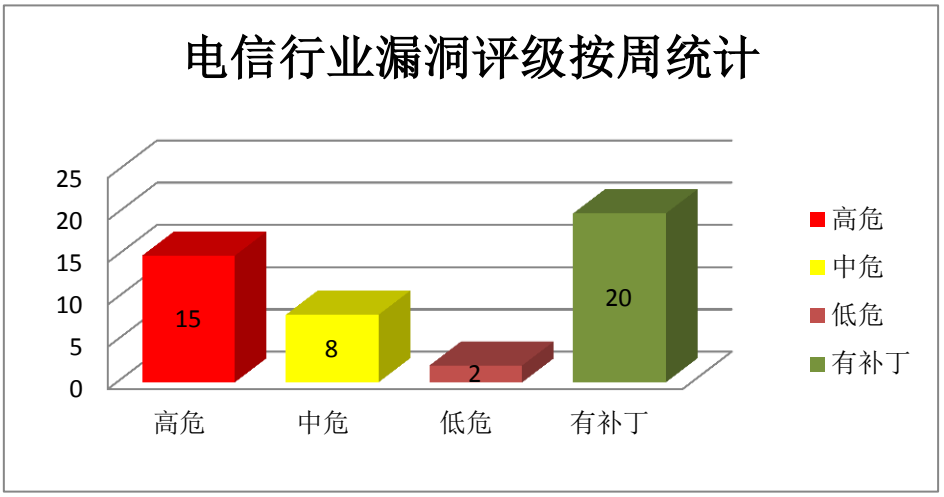

图 3 电信行业漏洞统计

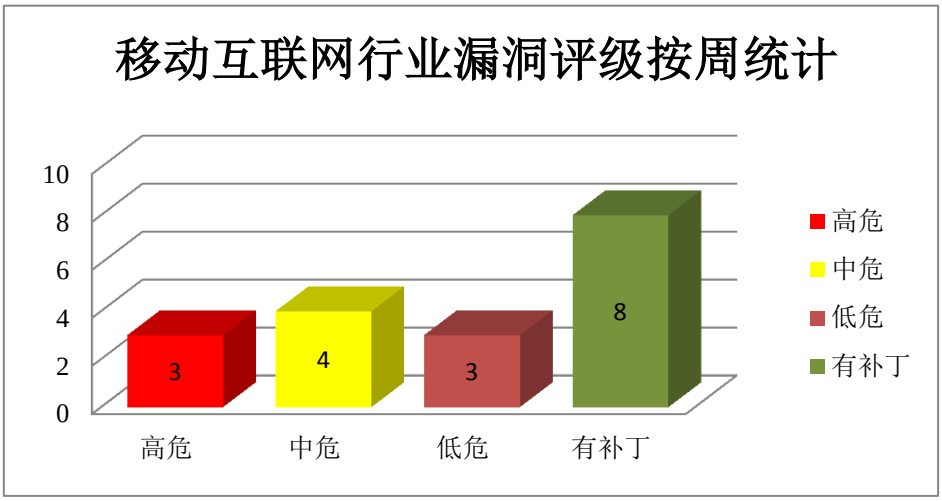

图 4 移动互联网行业漏洞统计

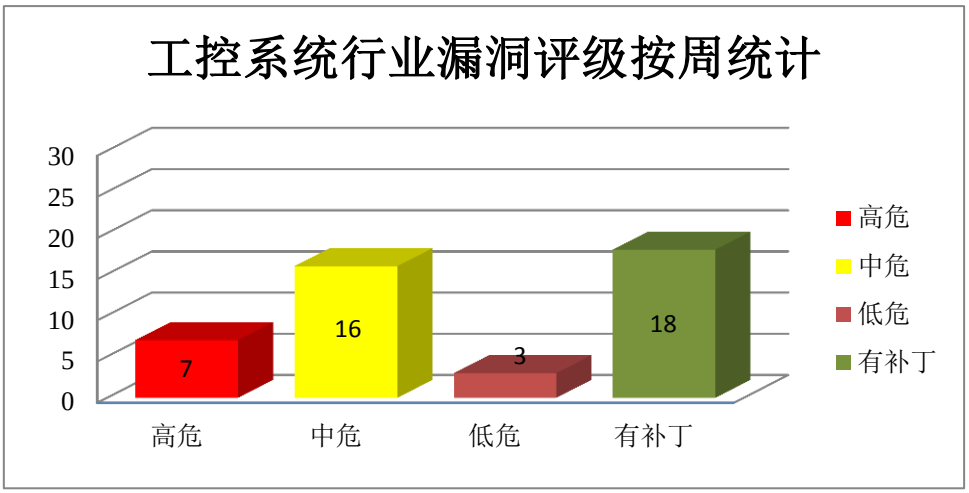

图 5 工控系统行业漏洞统计

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 Application Inspector 是一款软件源代码分析工具。Microsoft Word 是一套 Office 套件中的文字处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2020-19010）、Microsoft DirectX 权限提升漏洞（CNVD-2020-19009）、Microsoft Windows Network Connections Service 权限提升漏洞（CNVD-2020-19012）、Microsoft Windows Graphics Device Interface 远程代码执行漏洞（CNVD-2020-19247）、Microsoft Word 远程代码执行漏洞（CNVD-2020-19248）、Microsoft Windows Win32k 权限

提升漏洞（CNVD-2020-19894）、Microsoft Application Inspector 远程代码执行漏洞、Microsoft Word 远程执行代码漏洞（CNVD-2020-19916）。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-2020-19010
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19009
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19012
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19247
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19248
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19894
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19911
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19916

2、IBM 产品安全漏洞

IBM Content Navigator 是一款 Web 客户机。IBM DataPower Gateway 是一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B 和云工作负载而设计的安全和集成平台。IBM DB2 是一套关系型数据库管理系统。IBM Watson IoT Message Gateway 是物联网解决方案。IBM WebSphere Application Server（WAS）是一款应用服务器产品。IBM Cloud Orchestrator 是一套为云管理解决方案。IBM Power System S922 等都是美国 IBM 公司的一款基于 Power 处理器的服务器设备。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，伪造系统上的用户，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Content Navigator 会话固定漏洞、IBM Content Navigator 信息泄露漏洞（CNVD-2020-19221）、IBM DataPower Gateway 信息泄露漏洞（CNVD-2020-19261）、IBM DB2 缓冲区溢出漏洞（CNVD-2020-19263）、IBM Watson IoT Message Gateway 代码执行漏洞、IBM WebSphere Application Server 权限提升漏洞（CNVD-2020-19862）、IBM Cloud Orchestrator 安全绕过漏洞、多款 IBM 产品缓冲区溢出漏洞。其中，除“IBM Content Navigator 信息泄露漏洞（CNVD-2020-19221）、IBM DataPower Gateway 信息泄露漏洞（CNVD-2020-19261）、多款 IBM 产品缓冲区溢出漏洞”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-2020-19220
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19221
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19261
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19263
https://www.cnvd.org.cn/flaw/show/CNVD-2020-19864

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19862

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19867

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19868

3、Cisco 产品安全漏洞

Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。Cisco FXOS Software 是一套运行在思科安全设备中的防火墙软件。Cisco IOS XR 是一套为其网络设备开发的操作系统。Cisco Webex Network Recording Player 是一款用于播放视频会议记录的播放器。Cisco SD-WAN Solution 是一套网络扩展解决方案。Cisco Data Center Network Manager（DCNM）是一套数据中心管理系统。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 root 权限，执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco FXOS, IOS XR 和 NX-OS Software 中 Cisco Discovery 协议拒绝服务漏洞、Cisco Webex Network Recording Player 和 Webex Player 输入验证错误漏洞、Cisco SD-WAN Solution software 权限许可和访问控制问题漏洞、Cisco SD-WAN Solution 缓冲区溢出漏洞（CNVD-2020-19235）、Cisco Data Center Network Manager 路径遍历漏洞、Cisco SD-WAN Solution vManage 跨站脚本漏洞、Cisco SD-WAN Solution vManage 命令注入漏洞、Cisco SD-WAN Solution 命令注入漏洞（CNVD-2020-19236）。其中“Cisco FXOS, IOS XR 和 NX-OS Software 中 Cisco Discovery 协议拒绝服务漏洞、Cisco Webex Network Recording Player 和 Webex Player 输入验证错误漏洞、Cisco Data Center Network Manager 路径遍历漏洞、Cisco SD-WAN Solution vManage 命令注入漏洞”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-2020-19227

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19233

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19231

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19235

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19239

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19237

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19238

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19236

4、Intel 产品安全漏洞

Intel(R) Graphics Driver 是英特尔公司的一款显卡驱动程序。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，提升权限或导致拒绝服务。

CNVD 收录的相关漏洞包括：Intel(R) Graphics Driver 越界写入漏洞、Intel(R) Graphics Driver 不正确默认权限漏洞（CNVD-2020-18645、CNVD-2020-18647）、Intel(R) Graphics Driver 不正确访问控制漏洞（CNVD-2020-18643）、Intel(R) Graphics Driver

不受控制搜索路径漏洞（CNVD-2020-18646、CNVD-2020-18650）、Intel(R) Graphics Driver 不当条件检查漏洞、Intel(R) Graphics Driver 访问控制不当漏洞。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-2020-18639
https://www.cnvd.org.cn/flaw/show/CNVD-2020-18645
https://www.cnvd.org.cn/flaw/show/CNVD-2020-18643
https://www.cnvd.org.cn/flaw/show/CNVD-2020-18646
https://www.cnvd.org.cn/flaw/show/CNVD-2020-18647
https://www.cnvd.org.cn/flaw/show/CNVD-2020-18649
https://www.cnvd.org.cn/flaw/show/CNVD-2020-18652
https://www.cnvd.org.cn/flaw/show/CNVD-2020-18650

5、Artica Pandora FMS 代码执行漏洞

Artica Pandora FMS 是一套监控系统。本周，Artica Pandora FMS 被披露存在代码执行漏洞。攻击者可通过文件存储库组件上载.php 文件利用该漏洞执行任意代码。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-2020-19515

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-2020-18980	D-Link DIR-867、DIR-878 和 DIR-882 HNAP 认证绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10157
CNVD-2020-19198	Google Chrome 内存错误引用漏洞（CNVD-2020-19198）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2020/03/stable-channel-update-for-desktop_18.html
CNVD-2020-19212	ASUS Asuswrt-Merlin 缓冲区溢出漏洞	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.asus.com
CNVD-2020-19223	Red Hat JBoss Application Server 信息泄露漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2012-1094

CNVD-2020-19580	RICOH SP C250DN 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://www.ricoh.com/info/2019/0823_1
CNVD-2020-19855	Mitsubishi Electric MELQIC IU1 TCP 功能缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mitsubishielectric.co.jp/psirt/vulnerability/pdf/2019-004.pdf
CNVD-2020-19914	Fortinet FortiSIEM 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://docs.fortinet.com/document/fortisiem/5.2.6/release-notes/760862/whats-new-in-5-2-6
CNVD-2020-19926	Advantech WebAccess 缓冲区溢出漏洞（CNVD-2020-19926）	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.advantech.com.cn/
CNVD-2020-19930	Micro Focus Service Manager Automation SQL 注入漏洞	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.microfocus.com/
CNVD-2020-19939	Apache Shiro 身份认证绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/rc64fb2336683feff3580c3c3a8b28e80525077621089641f2f386b63@%3Ccommits.camel.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，执行任意代码。此外 IBM、Cisco、Intel 等多款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，伪造系统上的用户，执行任意代码，造成拒绝服务等。另外，Artica Pandora FMS 被披露存在代码执行漏洞。攻击者可通过文件存储库组件上载.php 文件利用该漏洞执行任意代码。

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、YzmCMS 'url'跨站脚本漏洞

验证描述

YzmCMS 是一款基于 PHP+Mysql 架构的轻量级开源内容管理系统,YzmCMS 可运行在 Linux、Windows、MacOSX、Solaris 等平台上。

YzmCMS 'url'存在跨站脚本漏洞。该漏洞是由于 Application/link/controller/link.class.php 文件中定义的 add 函数未能过滤过滤 url 参数，导致执行恶意代码执行恶意代码。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35075

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-18978

信息提供者

CNVD 工作组

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. 严重的 RCE 漏洞影响了数百万基于 OpenWrt 的网络设备

一位安全研究人员披露了影响基于 OpenWrt Linux 操作系统的网络设备的严重远程执行代码漏洞。该漏洞被命名为 CVE-2020-7982，存在于 OpenWrt 的 OPKG 软件包管理器中。

参考链接：https://securityaffairs.co/wordpress/100400/hacking/critical-rce-openwrt-devices.html

2. 攻击者利用通达 OA 漏洞释放勒索病毒，用户数据遭到加密

近日，通达 OA 官方论坛发布了一则安全更新，披露了近期出现攻击者利用通达 OA 文件上传和文件包含漏洞释放勒索病毒的攻击事件，攻击者通过漏洞上传 webshell 伪装 OA 插件的下载提示页面，诱导用户点击下载运行勒索病毒，官方紧急发布了各版本的安全加固补丁。从官方发布的补丁分析，通达 OA V11 以下版本仅存在未授权任意文件上传漏洞；通达 OA V11 版本则存在未授权任意文件上传以及任意文件包含两个漏洞，攻击者可在通达 OA V11 版本利用两个漏洞构造组合利用链，最终在目标服务器上执行任意代码。

参考链接：https://www.freebuf.com/vuls/230909.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