国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 04 月 13 日-2020 年 04 月 19 日　　2020 年第 16 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 419 个，其中高危漏洞 204 个、中危漏洞 182 个、低危漏洞 33 个。漏洞平均分值为 6.81。本周收录的漏洞中，涉及 0day 漏洞 190 个（占 45%），其中互联网上出现“D-Link DWL-2600 认证远程命令注入漏洞、Windscribe 权限提升漏洞”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 4486 个，与上周（2497 个）环比增加 79%。

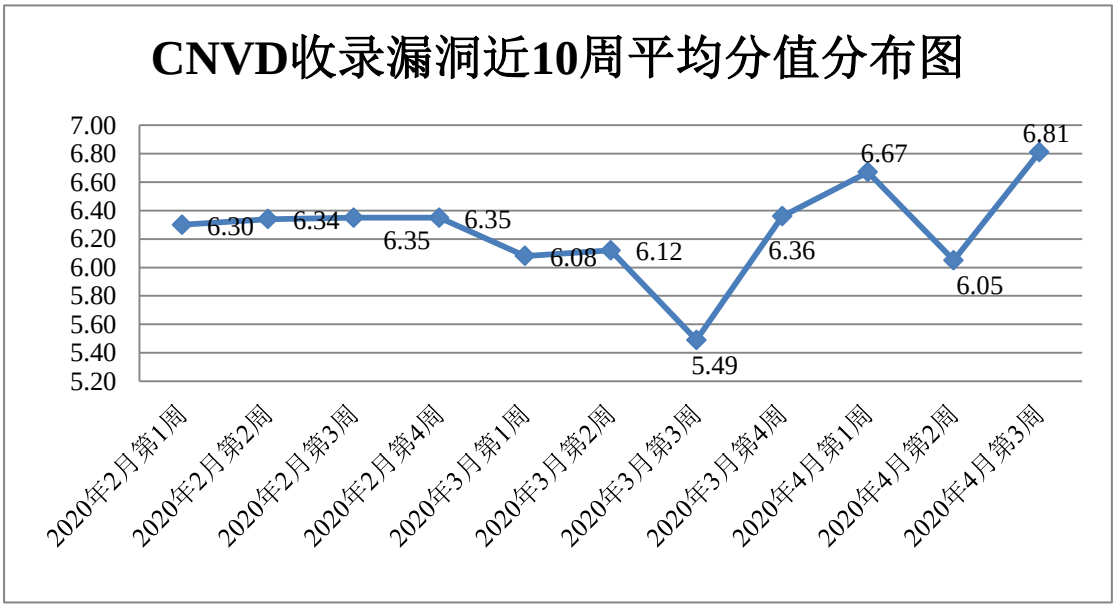

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 11 起，向基础电信企业通报漏洞事件 2 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 245 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 31 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 9 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：

福州富昌维控电子科技有限公司、北京亚控科技发展有限公司、灵宝简好网络科技有限公司、北京国炬信息技术有限公司、上海复旦天翼计算机有限公司、石家庄市征红网络科技有限公司、长沙德尚网络科技有限公司、广州虹科电子科技有限公司、北京世纪超星信息技术发展有限责任公司、长沙友点软件科技有限公司、上海顶想信息科技有限公司、上海卓卓网络科技有限公司、恒泰证券股份有限公司、安科讯（福建）科技有限公司、北京猎豹移动科技有限公司、科汛软件有限公司、上海广乐网络科技有限公司、广州市三今网络技术有限公司、上海丹帆网络科技有限公司、北京酷我科技有限公司、广州虎牙信息科技有限公司、广州酷狗计算机科技有限公司、北京风行在线技术有限公司、北京力控元通科技有限公司、长沙米拓信息技术有限公司、湖南壹拾捌号网络技术有限公司、北京百卓网络技术有限公司、合肥奇乐网络科技有限公司、宿迁鑫潮信息技术限公司、廊坊市极致网络科技有限公司、苏州托普斯网络科技有限公司、友讯电子设备（上海）有限公司、广州虹科电子科技有限公司、广州优天网络科技有限公司、上海亿速网络科技有限公司、哈尔滨伟成科技有限公司、深圳市迅雷网络技术有限公司、深圳云安宝科技有限公司、普联软件股份有限公司、昆明云涛科技有限公司、上海二三四五网络科技有限公司、浙江核新同花顺网络信息股份有限公司、罗克韦尔自动化（中国）有限公司、珠海金山办公软件有限公司、通用电气（GE）公司、深圳市成为信息技术有限公司、西安佰联网络技术有限公司、猪八戒股份有限公司、北京天恒昕业科技发展有限公司、广东凯格科技有限公司、深圳市零壹贰科技有限公司、台州企诚网络科技有限公司、深圳市博士通科技有限公司、龙采科技集团有限责任公司、苏州万户网络科技有限公司、许昌永诚网络科技有限公司、随身学有限公司、北京墨砚聚客文化传播有限公司、宁波慕枫网络科技有限公司、湖南翱云网络科技有限公司、北京智量科技有限公司、南京蓝鲸人网络科技有限公司、武汉勾勾互娱科技有限公司、网易有道信息技术（北京）有限公司、深圳市腾讯计算机系统有限公司、广州市风荷科技有限公司、福建福昕软件开发股份有限公司、上海荃路软件开发工作室、新秀工作室、北京为因软件、中瑞网络、石家庄金翼网络工作室、伟创互联网络技术开发团队、逍遥 B2C 商城系、贴心猫(imcat)、施耐德（Schneider Electric）、万通 CMS、海洋 CMS 、狂雨小说 cms、WMCMS 团队、Freecms、Fiyo CMS、Valine、Oracle Corporation、UQCMS、BEESCMS、MicroDicom、MessageSolution、JunAMS、MayiCMS、115cms、PopojiCMS、MongoDB、Joomla！和 XDCMS。

本周，CNVD 发布了《Microsoft 发布 2020 年 4 月安全更新》、《Oracle 发布 2020 年 4 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5487

https://www.cnvd.org.cn/webinfo/show/5489

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、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。北京铭图天成信息技术有限公司、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、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、国瑞数码零点实验室、上海观安信息技术股份有限公司、杭州迪普科技股份有限公司、内蒙古洞明科技有限公司、浙江国利网安科技有限公司、博智安全科技股份有限公司、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、北京信联科汇科技有限公司、北京安信天行科技有限公司、山东云天安全技术有限公司、四川哨兵信息科技有限公司、天津市兴先道科技有限公司、河南信安世纪科技有限公司、广州安亿信软件科技有限公司、成都安美勤信息技术股份有限公司、北京冠程科技有限公司、北京智游网安科技有限公司、北京浩瀚深度信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 4486 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 3775 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）	1888	1888
上海交大	1142	1142
奇安信网神（补天平台）	745	745
恒安嘉新(北京)科技股份公司	540	0
华为技术有限公司	295	0
哈尔滨安天科技集团股份有限公司	245	0
北京天融信网络安全技术有限公司	179	6
深信服科技股份有限公司	107	0
北京神州绿盟科技有限公司	85	2

北京启明星辰信息安全技术有限公司	72	18
新华三技术有限公司	58	0
北京数字观星科技有限公司	38	0
杭州安恒信息技术股份有限公司	26	26
厦门服云信息科技有限公司	24	0
北京知道创宇信息技术股份有限公司	20	9
北京奇虎科技有限公司	14	0
沈阳东软系统集成工程有限公司	3	3
南京铱迅信息技术股份有限公司	1	1
北京铭图天成信息技术有限公司	102	102
北京华云安信息技术有限公司	74	74
南京众智维信息科技有限公司	46	46
河南灵创电子科技有限公司	44	44
远江盛邦（北京）网络安全科技股份有限公司	33	33
长春嘉诚信息技术股份有限公司	26	26
国瑞数码零点实验室	26	26
上海观安信息技术股份有限公司	17	17
杭州迪普科技股份有限公司	12	0
内蒙古洞明科技有限公司	8	8
浙江国利网安科技有限公司	8	8
博智安全科技股份有限公司	6	6
山东新潮信息技术有限公司	6	6

北京圣博润高新技术股份有限公司	5	5
北京信联科汇科技有限公司	3	3
北京安信天行科技有限公司	2	2
山东云天安全技术有限公司	2	2
四川哨兵信息科技有限公司	2	2
天津市兴先道科技有限公司	2	2
河南信安世纪科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
北京冠程科技有限公司	1	1
北京智游网安科技有限公司	1	1
北京浩瀚深度信息技术股份有限公司	1	1
CNCERT 西藏分中心	1	1
CNCERT 广西分中心	1	1
CNCERT 青海分中心	1	1
个人	225	225
报送总计	6140	4486

本周漏洞按类型和厂商统计

本周，CNVD 收录了 419 个漏洞。应用程序 205 个，WEB 应用 109 个，网络设备（交换机、路由器等网络端设备）39 个，操作系统 39 个，安全产品 16 个，数据库 7 个，智能设备（物联网终端设备）4 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	205
WEB 应用	109
网络设备（交换机、路由器等网络端设备）	39
操作系统	39
安全产品	16
数据库	7
智能设备（物联网终端设备）漏洞	4

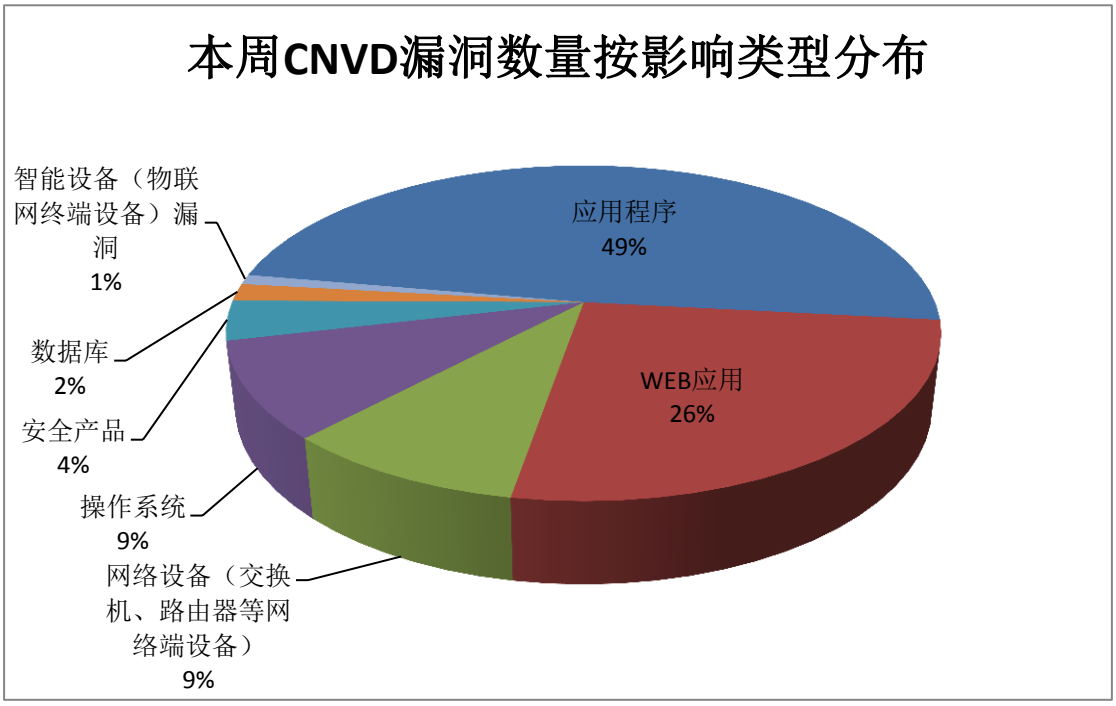

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Apple、WordPress 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	21	5%
2	Apple	19	5%
3	WordPress	16	4%
4	IBM	14	3%
5	NETGEAR	13	3%
6	Oracle	12	3%
7	Juniper Networks	8	2%
8	Linux	6	1%
9	Dell	6	1%

10	其他	304	73%

本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，22 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“D-Link DSL-GS225 J1 操作系统命令注入漏洞、TP-Link TL-WR841N 缓冲区溢出漏洞（CNVD-2020-23185）、Apple macOS Catalina Apple GraphicsControl 组件内存破坏漏洞、多款 Siemens 产品资源管理错误漏洞”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/

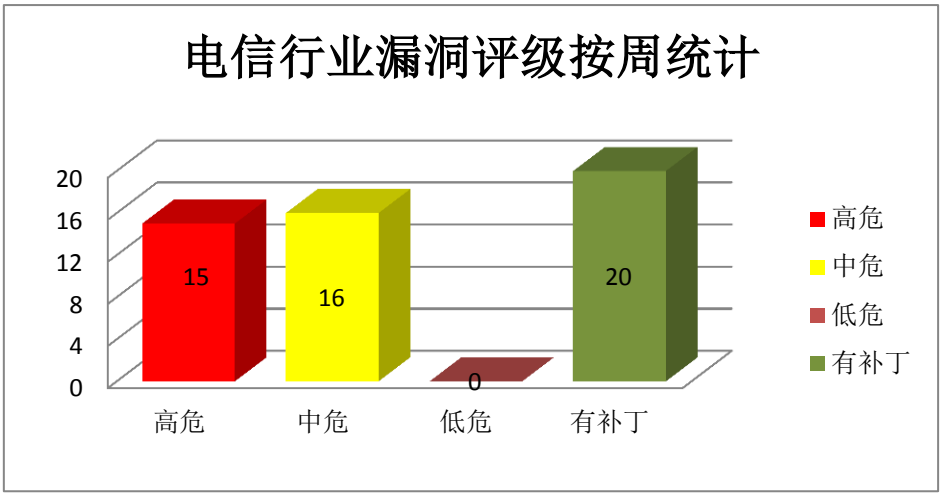

图 3 电信行业漏洞统计

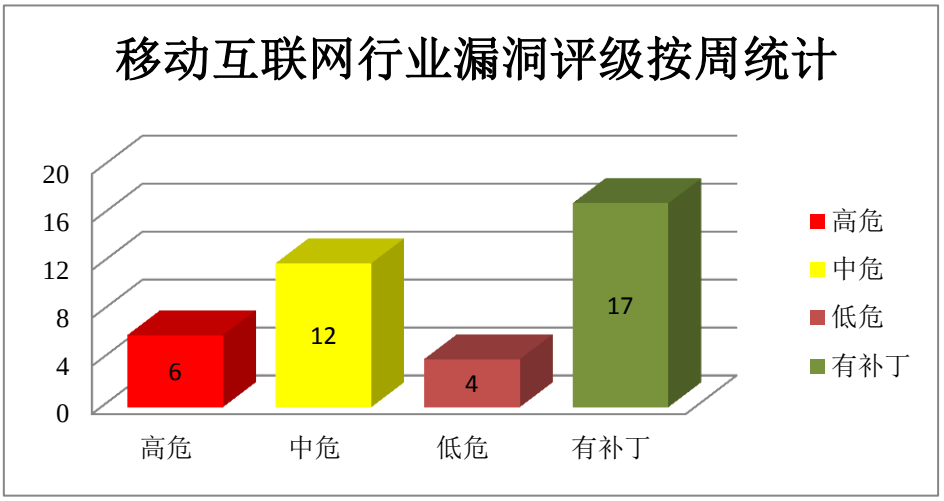

图 4 移动互联网行业漏洞统计

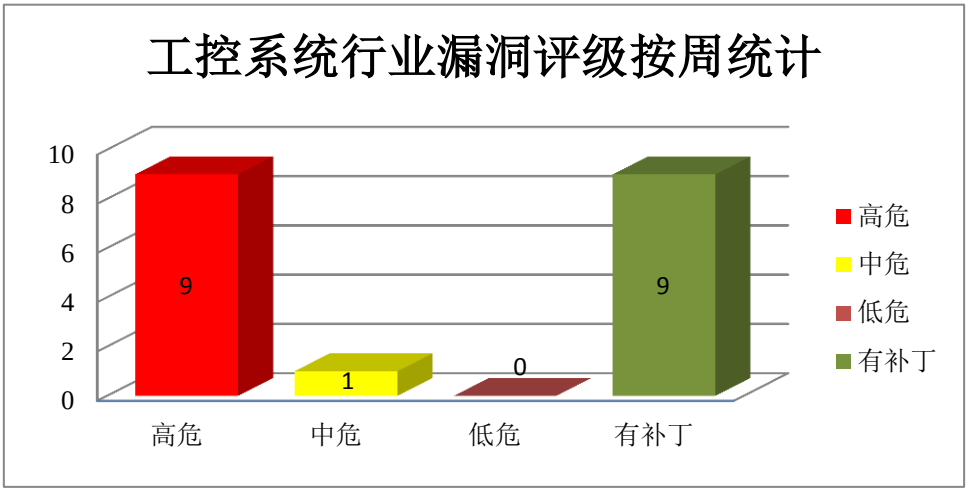

图 5 工控系统行业漏洞统计

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、Apple 产品安全漏洞

Apple macOS Catalina 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，或造成系统意外终止或读取内核内存。

CNVD 收录的相关漏洞包括：Apple macOS Catalina Bluetooth 组件内存破坏漏洞（CNVD-2020-22464、CNVD-2020-22469、CNVD-2020-23217）、Apple macOS Catalina Bluetooth 组件缓冲区溢出漏洞（CNVD-2020-22473、CNVD-2020-23213、CNVD-2020-23212）、Apple macOS Catalina Apple HSSPI Support 组件内存破坏漏洞、Apple macOS Catalina AppleGraphicsControl 组件内存破坏漏洞。其中，除“Apple macOS Catalina Bluetooth 组件缓冲区溢出漏洞（CNVD-2020-22473、CNVD-2020-23213、CNVD-2020-23212）”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-2020-22464

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22467

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22473

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22470

https://www.cnvd.org.cn/flaw/show/CNVD-2020-22469

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23213

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23212

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23217

2、WordPress 产品安全漏洞

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。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，执行客户端代码，导致网站无法访问等。

CNVD 收录的相关漏洞包括：WordPress Contact Form 7 Datepicker 跨站脚本漏洞、WordPress LifterLMS 插件代码问题漏洞、WordPress 301 Redirects-Easy Redirect Manager 数据伪造问题漏洞、WordPress all-in-one-seo-pack 插件跨站脚本漏洞、WordPress ultimate-faqs 插件输入验证错误漏洞、WordPress Media Library Assistant 信息泄露漏洞、WordPress Responsive Poll 授权问题漏洞、WordPress Snap Creek Duplicator 和 Duplicator Pro 路径遍历漏洞。其中，除“WordPress Contact Form 7 Datepicker 跨站脚本漏洞、WordPress all-in-one-seo-pack 插件跨站脚本漏洞”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-2020-22665
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22669
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22693
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22702
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22699
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22848
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22850
https://www.cnvd.org.cn/flaw/show/CNVD-2020-22857

3、IBM 产品安全漏洞

IBM QRadar SIEM 是美国 IBM 公司的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。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。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，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM QRadar SIEM 信息泄露漏洞（CNVD-2020-23040、CNVD-2020-23041、CNVD-2020-23044）、IBM QRadar SIEM 跨站脚本漏洞（CNVD-2020-23043）、IBM QRadar SIEM 文件上传漏洞、IBM QRadar SIEM 命令执行漏洞、IBM QRadar SIEM 权限提升漏洞、IBM QRadar SIEM 服务器端请求伪造漏洞（CNVD-2020-23049）。其中“IBM QRadar SIEM 文件上传漏洞、IBM QRadar SIEM 命令执行漏洞、IBM QRadar SIEM 权限提升漏洞、IBM QRadar SIEM 服务器端请求伪造漏洞（CNVD-2020-23049）”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-2020-23040
https://www.cnvd.org.cn/flaw/show/CNVD-2020-23043

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23041

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23047

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23046

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23045

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23044

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23049

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 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。DirectX 是其中的一个多媒体系统链接库。Windows Hyper-V 是其中的一个虚拟化产品，支持在 Windows 中创建虚拟机。Windows Jet Database Engine 是其中的一个数据库引擎。Microsoft Office 是一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、FrontPage 等。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。ChakraCore 是使用在 Edge 浏览器中的一个开源的 ChakraJavaScript 脚本引擎的核心部分，也可作为单独的 JavaScript 引擎使用。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，攻击者可利用漏洞执行任意代码，破坏内存。

CNVD 收录的相关漏洞包括：Microsoft Windows DirectX 提权漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2020-23435）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2020-23433）、Microsoft Windows Jet Database Engine 远程代码执行漏洞（CNVD-2020-23432）、Microsoft Office 远程执行代码漏洞（CNVD-2020-23440）、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2020-23445）、Microsoft Internet Explorer VBScript Engine 远程执行代码漏洞、Microsoft Edge 内存破坏漏洞（CNVD-2020-23446）。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-2020-23430

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23435

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23433

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23432

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23440

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23445

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23444

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23446

5、Cisco Webex Meetings 访问控制错误漏洞

Cisco Webex Meetings 是美国思科（Cisco）公司的一套视频会议解决方案。本周，

Cisco Webex Meetings 被披露存在访问控制错误漏洞。该漏洞源于当会议室主持人查看共享的多媒体文件时不会弹出安全警告对话框。远程攻击者可借助主持人身份共享文件并诱使之前的主持人浏览该多媒体文件利用该漏洞绕过安全限制。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-2020-22854

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-2020-22676	Lenovo ThinkPad 产品输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.lenovo.com/us/en/product_security/LEN-27714
CNVD-2020-22684	Barco ClickShare Button R9861500D01 代码问题漏洞	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.barco.com
CNVD-2020-22703	GitLab 远程代码执行漏洞（CNVD-2020-22703）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://about.gitlab.com/2019/08/12/critical-security-release-gitlab-12-dot-1-dot-6-released/
CNVD-2020-22855	Google Chrome 代码执行漏洞（CNVD-2020-22855）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://chromereleases.googleblog.com/2020/04/stable-channel-update-for-desktop_7.html
CNVD-2020-22957	Palo Alto Networks PAN-OS 格式化字符串错误漏洞（CNVD-2020-22957）	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.paloaltonetworks.com/CVE-2020-1992
CNVD-2020-22965	Dell EMC Networking X-Series 、Dell EMC Networking PC5500 和 Dell EMC PowerEdge VRTX Switch Modules 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://www.dell.com/support/article/en-us/sln320366/dsa-2020-042-dell-networking-security-update-for-an-information-disclosure-vulnerability?lang=en
CNVD-2020-23015	Oracle Fusion Middleware WebLogic Server 远程代码执行漏洞（CNVD-2020-23015）	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.oracle.com/security-alerts/cpuapr2020.html
CNVD-2020-	Eclipse Che 未授权访问漏洞	高	目前厂商已发布升级补丁以修复漏

23231			洞，详情请关注厂商主页：https://www.eclipse.org/
CNVD-2020-23238	ZOHO ManageEngine ADSelfService Plus 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/community/topic/adselfservice-plus-5815-released-with-an-important-security-fix
CNVD-2020-23405	GPAC 资源管理错误漏洞（CNVD-2020-23405）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/gpac/gpac/issues/1440

小结：本周，Apple 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，或造成系统意外终止或读取内核内存。此外 WordPress、IBM、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敏感信息，提升权限，执行任意代码等。另外，Cisco Webex Meetings 被披露存在访问控制错误漏洞。攻击者可借助主持人身份共享文件并诱使之前的主持人浏览该多媒体文件利用该漏洞绕过安全限制。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、D-Link DWL-2600 认证远程命令注入漏洞

验证描述

D-Link DWL-2600 是一款无线接入点设备。

D-Link DWL-2600 存在安全漏洞。攻击者可利用漏洞注入任意命令。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35272

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-22738

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. 福特、大众畅销车曝安全漏洞，黑客可窃取隐私、操控车辆

近日，一份来自英国消费者协会杂志《Which?》调查报告发现，福特和大众的两款畅销车存在严重安全漏洞，黑客可利用该漏洞发动攻击，窃取车主的个人隐私信息，甚至是操控车辆，对车主的信息安全和生命安全产生极大的威胁。

参考链接：https://www.freebuf.com/news/233955.html

2. 恶意 URL 可能会导致 Git 将存储的凭据提供给错误的服务器

Git 使用外部的“凭证帮助程序”来存储和检索操作系统提供的安全存储中的密码或其他凭证。包含编码换行符的特制 URL 可以将意想不到的值注入到凭据帮助程序协议流中，从而导致凭据帮助程序检索一个服务器（例如 good.example.com）的密码，并向另一个服务器（例如 evil.example.com）发出 HTTP 请求，结果将前者的凭据发送给后者。

参考链接：https://github.com/git/git/security/advisories/GHSA-qm7j-c969-7j4q

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