国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 01 月 20 日-2020 年 02 月 02 日　　2020 年第 4、5 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 221 个，其中高危漏洞 51 个、中危漏洞 145 个、低危漏洞 25 个。漏洞平均分值为 5.34。本周收录的漏洞中，涉及 0day 漏洞 56 个（占 25%），其中互联网上出现“WordPress Import Legacy Media 跨站脚本漏洞、WordPress Movies 跨站脚本漏洞”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 933 个，与上周（2126 个）环比减少 56%。

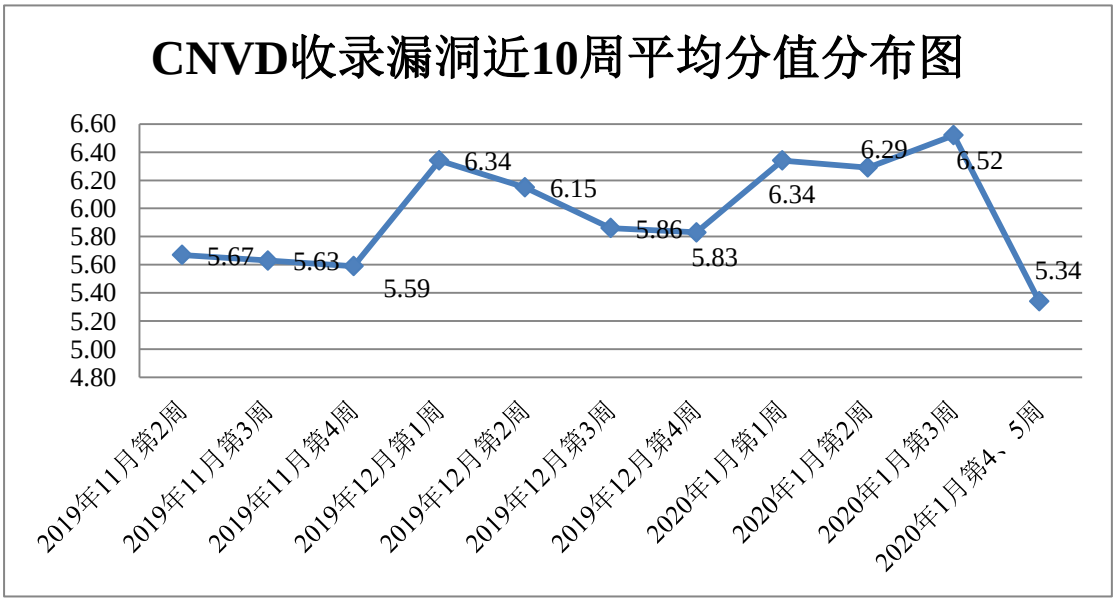

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 18 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 200 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 12 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 29 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：

汕头市三互科技有限公司、镇江市云优网络科技有限公司、北京智量科技有限公司、深圳市昂捷信息技术股份有限公司、大连船舶重工集团海洋工程有限公司、长沙德尚网络科技有限公司、北京天地华大网络技术有限公司、中国船舶重工集团国际工程有限公司、廊坊市极致网络科技有限公司、甲骨文股份有限公司、中国普法教育网和梦想 CMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、京神州绿盟科技有限公司、为技术有限公司等单位报送公开收集的漏洞数量较多。内蒙古奥创科技有限公司、京铭图天成信息技术有限公司、南灵创电子科技有限公司、瑞数码零点实验室、江盛邦（北京）网络安全科技股份有限公司、州迪普科技股份有限公司、蒙古洞明科技有限公司、京圣博润高新技术股份有限公司、石网科通信技术股份有限公司、东云天安全技术有限公司、南信安世纪科技有限公司、门靠谱云股份有限公司、海端御信息科技有限公司、州学院网络与信息安全研究所、春嘉诚信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 933 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 571 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
阿里云计算有限公司	787	0
奇安信网神（补天平台）	458	458
上海交大	112	112
北京神州绿盟科技有限公司	81	5
华为技术有限公司	47	0
北京数字观星科技有限公司	20	0
新华三技术有限公司	20	0

斗象科技（漏洞盒子）	1	1
内蒙古奥创科技有限公司	32	32
北京铭图天成信息技术有限公司	30	30
河南灵创电子科技有限公司	19	19
国瑞数码零点实验室	16	16
远江盛邦（北京）网络安全科技股份有限公司	15	15
杭州迪普科技股份有限公司	14	0
内蒙古洞明科技有限公司	8	8
北京圣博润高新技术股份有限公司	6	6
山石网科通信技术股份有限公司	4	4
山东云天安全技术有限公司	3	3
河南信安世纪科技有限公司	2	2
厦门靠谱云股份有限公司	1	1
上海端御信息科技有限公司	1	1
梧州学院网络与信息安全研究所	1	1
长春嘉诚信息技术股份有限公司	1	1
CNCERT 天津分中心	15	15
CNCERT 上海分中心	14	14
CNCERT 海南分中心	5	5
CNCERT 吉林分中心	1	1
个人	183	183
报送总计	1897	933

本周漏洞按类型和厂商统计

本周，CNVD 收录了 221 个漏洞。应用程序 133 个，WEB 应用 28 个，操作系统 25 个，智能设备（物联网终端设备）19 个，网络设备（交换机、路由器等网络端设备）10 个，安全产品 4 个，数据库 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	133
WEB 应用	28
操作系统	25
智能设备（物联网终端设备）	19
网络设备（交换机、路由器等网络端设备）	10
安全产品	4
数据库	2

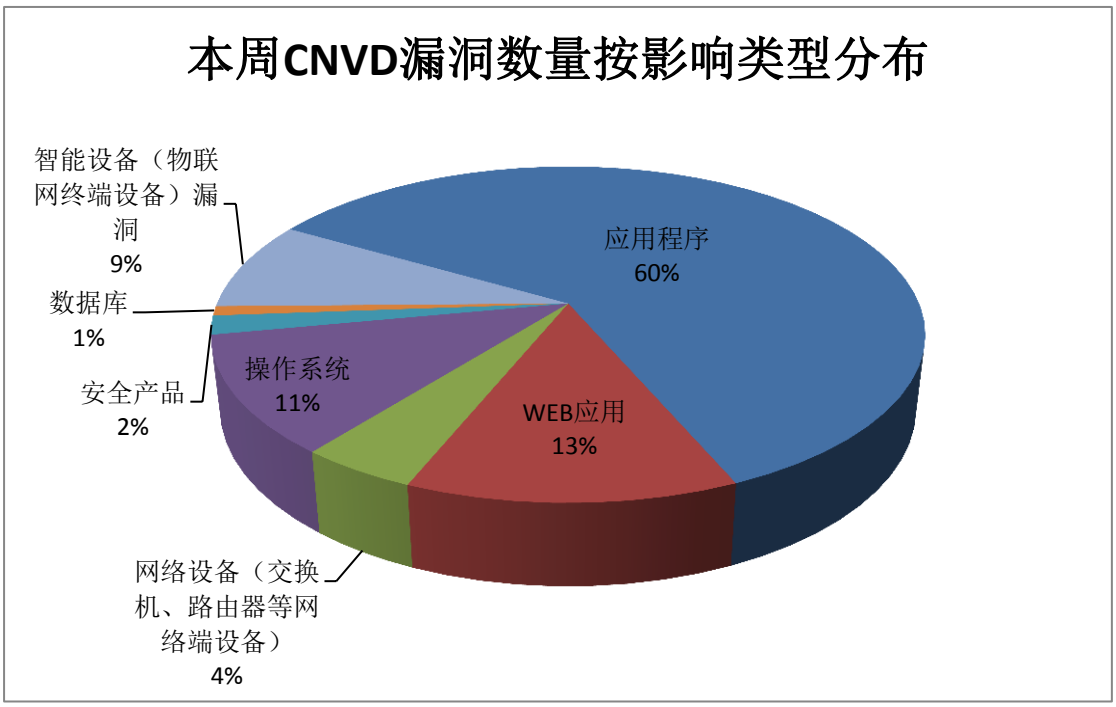

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Huawei、Oracle 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	WordPress	16	7%
2	Huawei	13	6%
3	Oracle	13	6%

4	Mozilla	12	5%
5	Red Hat	12	5%
6	Apple	16	7%
7	Google	10	5%
8	GitLab	8	4%
9	Adobe	7	3%
10	其他	114	52%

本周行业漏洞收录情况

本周，CNVD 收录了 7 个电信行业漏洞，11 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Moxa EDS-G508E, EDS-G512E, and EDS-G516E Series Ethernet Switches 资源管理错误漏洞、Apple iOS 和 Apple macOS Mojave IOKit SCSI 组件内存破坏漏洞、Advantech DiagAnywhere Server 缓冲区溢出漏洞、多款 Apple 产品 MobileLockdown 组件权限提升漏洞”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/

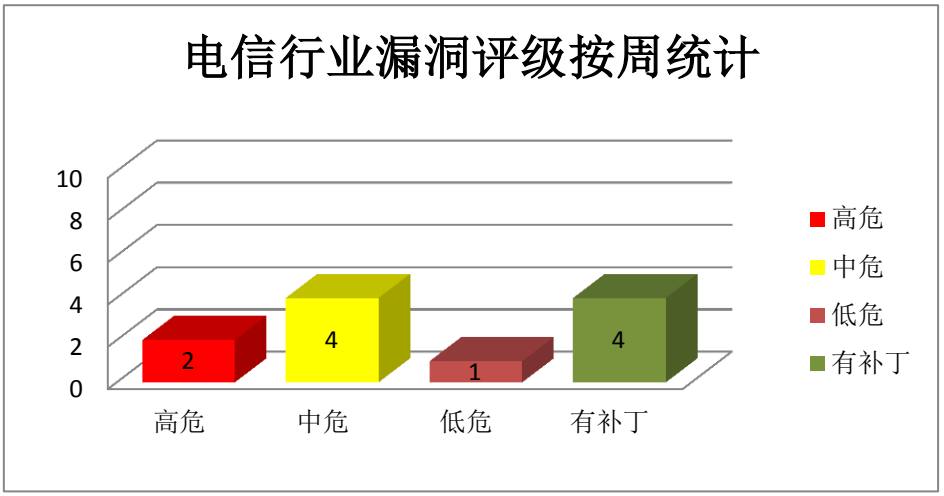

图 3 电信行业漏洞统计

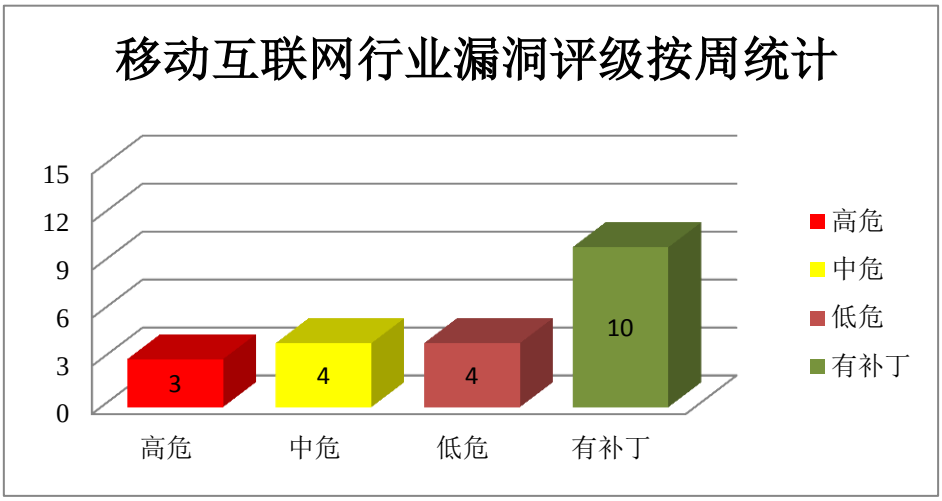

图 4 移动互联网行业漏洞统计

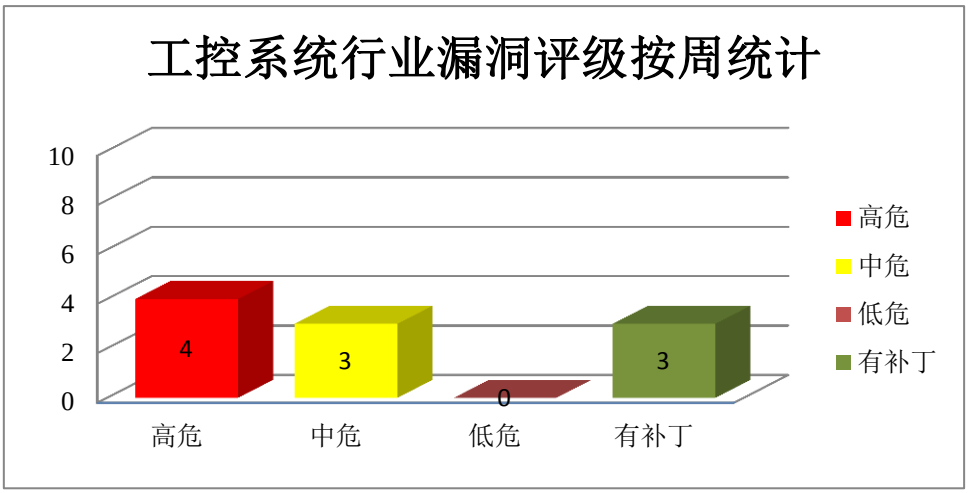

图 5 工控系统行业漏洞统计

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、Huawei 产品安全漏洞

Huawei Honor V10 是一款智能手机产品。Mate 10 Pro 是一款智能手机。Huawei Mate 20 Pro 是一款智能手机。Huawei AR1200 是一款企业路由器。Huawei S12700 是一款企业级交换机产品。Huawei P30 是一款智能手机。Huawei P30 Pro 是一款智能手机。Huawei M6 是一款平板电脑。Huawei Gauss100 OLTP 是一款华为的数据库系统。Huawei Honor V30 是一款智能手机。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未授权的操作，获取敏感信息，导致拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Huawei 产品拒绝服务漏洞（CNVD-2020-02948）、Huawei Mate 20 Pro 授权问题漏洞、多款 Huawei 产品信息泄露漏洞（CNVD-2020-02963）、多款 Huawei 产品加密问题漏洞、多款 Huawei 产品数据伪造问题漏洞、多款 Hua

wei 产品路径遍历漏洞、Huawei Gauss100 OLTP 数据库缓冲区溢出漏洞、Huawei Honor V30 授权问题漏洞。其中，“多款 Huawei 产品拒绝服务漏洞（CNVD-2020-02948）”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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-02948
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02962
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02963
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02964
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02965
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02966
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02967
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02968

2、Apple 产品安全漏洞

Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple macOS Mojave 是一套专为 Mac 计算机所开发的专用操作系统。Apple Shortcuts for iOS 是一套基于 iOS 平台的快捷应用。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过沙盒限制，提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：多款 Apple 产品 TrueTypeScaler 组件越界读取漏洞、Apple iOS IOKit 内存破坏漏洞、Apple iOS 和 Apple macOS Mojave IOKit SCSI 组件内存破坏漏洞、Apple macOS Mojave AMD 组件内存破坏漏洞、多款 Apple 产品 MobileLockdown 组件权限提升漏洞、Apple Shortcuts for iOS 沙盒限制绕过漏洞、多款 Apple 产品 Audio 组件缓冲区溢出漏洞、Apple macOS Mojave Intel Graphics Driver 组件任意代码执行漏洞（CNVD-2020-03212）。其中，除“多款 Apple 产品 TrueTypeScaler 组件越界读取漏洞、多款 Apple 产品 Audio 组件缓冲区溢出漏洞”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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03001
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03004
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03003
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03008
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03009
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03006
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03034
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03212

3、GitLab 产品安全漏洞

GitLab 是一款使用 Ruby on Rails 开发的、自托管的、Git（版本控制系统）项目仓库应用程序。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未授权的访问权限，造成拒绝服务等。

CNVD 收录的相关漏洞包括：GitLab 代码问题漏洞（CNVD-2020-03032）、GitLab 资源管理错误漏洞（CNVD-2020-03053）、GitLab 访问控制错误漏洞（CNVD-2020-03058）、GitLab CE/EE 信息泄露漏洞（CNVD-2020-03114）、GitLab CE/EE 跨站脚本漏洞（CNVD-2020-03115）、GitLab 访问控制错误漏洞（CNVD-2020-03229）、GitLab 未授权访问漏洞（CNVD-2020-03230）、GitLab 拒绝服务漏洞（CNVD-2020-03231）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03032
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03053
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03058
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03114
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03115
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03229
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03230
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03231

4、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过内容安全策略限制，提升权限，执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 内存破坏漏洞（CNVD-2020-02973）、Mozilla Firefox 安全绕过漏洞（CNVD-2020-02975）、Mozilla Firefox 代码执行漏洞（CNVD-2020-02976）、多款 Mozilla 产品权限提升漏洞、Mozilla Firefox 拒绝服务漏洞（CNVD-2020-03210）、Mozilla Firefox 输入验证错误漏洞（CNVD-2020-03243）、多款 Mozilla 产品缓冲区溢出漏洞（CNVD-2020-03240）、多款 Mozilla 产品内存破坏漏洞（CNVD-2020-03241）。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-02973
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02975
http://www.cnvd.org.cn/flaw/show/CNVD-2020-02976
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03209
http://www.cnvd.org.cn/flaw/show/CNVD-2020-03210

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03243

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03240

http://www.cnvd.org.cn/flaw/show/CNVD-2020-03241

5、Sony Catalyst Production Suite 和 Catalyst Browse 权限提升漏洞

Sony catalyst production suite 是由索尼推出的一款视频编辑处理套件，该套件其实是包含了 atalyst Edit 和 Catalyst Prepare 两个组件。Sony Catalyst Browse 是一个媒体管理软件。本周，Sony Catalyst Production Suite 2019.1 (1.1.0.21)及之前版本和 Catalyst Browse 2019.1 (1.1.0.21)及之前版本被披露存在限提升漏洞。攻击者可利用该漏洞获取管理员权限并以该权限运行程序。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：http://www.cnvd.org.cn/flaw/show/CNVD-2020-03065

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-2020-02993	PrestaShop Adobe Stock API integration 文件上传漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.prestashop.com
CNVD-2020-02997	Adobe Illustrator CC 2019 内存破坏漏洞	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/experience-manager/apsb20-01.html
CNVD-2020-03014	DTEN D5 和 DTEN D7 代码执行漏洞	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.displayten.com.cn/
CNVD-2020-03041	Microsoft Windows Win32k 组件权限提升漏洞（CNVD-2020-03041）	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/zh-CN/security-guidance/advisory/CVE-2019-1458
CNVD-2020-03060	Sangoma Technologies Asterisk 和 Sangoma Technologies Certified Asterisk 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://downloads.asterisk.org/pub/security
CNVD-2020-03119	libsixel 内存泄漏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/saitoha/libsixel/commit/b9a4175c803b50a863b0fbd8b8b49058ca725ea6

CNVD-2020-03162	Dell RSA Identity Governance and Lifecycle 和 RSA Via Lifecycle and Governance 访问控制错误漏洞	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.dell.com/support/security/zh-cn/details/DOC-109310/DSA-2019-164-RSA-Identity-Governance-and-Lifecycle-Product-Security-Update-for-Multiple-Vulnerabi
CNVD-2020-03183	VMware ESXi 和 VMware Horizon DaaS OpenSLP 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.vmware.com/security/advisories/VMSA-2019-0022.html
CNVD-2020-03190	TI-Tool TITool PrintMonitor SQL 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://www.titool.eu
CNVD-2020-03191	Advantech DiagAnywhere Server 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.advantech.com

小结：本周，Huawei 产品被披露存在多个漏洞，攻击者可利用漏洞进行未授权的操作，获取敏感信息，导致拒绝服务等。此外，Apple、GitLab、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过内容安全策略限制，获取未授权的访问权限，提升权限，执行任意代码，造成拒绝服务等。另外，Sony Catalyst Production Suite 和 Catalyst Browse 被披露存在权限提升漏洞。攻击者可利用该漏洞获取管理员权限并以该权限运行程序。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、WordPress Import Legacy Media 跨站脚本漏洞

验证描述

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。Import Legacy Media 是使用在其中的一个媒体文件导入插件。

WordPress Import Legacy Media 0.1 及之前版本中存在跨站脚本漏洞，该漏洞源于 WEB 应用缺少对客户端数据的正确验证，攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://codevigilant.com/disclosure/wp-plugin-import-legacy-media-a3-cross-site-scripting-xss/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-02954

信息提供者

哈尔滨安天科技集团股份有限公司

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. 乌克兰政府招聘官网曝出网络安全事件：求职人员的诸多详细信息被泄漏

乌克兰政府招聘门户官网近日被爆出现公民信息被泄漏事件，当地官员声称他们已经发现并修复了他们所说的“漏洞”。乌克兰政府使用 https://career.gov.ua/ 这个门户网站来发布政府岗位招募信息，并要求申请人提交各种身份证明信息，包括全名，地址，身份证件扫描，护照扫描件，文凭和其他毕业文件。

参考链接：https://www.cnbeta.com/articles/tech/934879.htm

2. 阿拉伯木马成功汉化，多款 APP 惨遭模仿用于攻击

近日，某病毒响应中心在日常样本监控过程中发现了一批伪装成点读通.apk、作业帮.apk、手机找回.apk、PUBG.apk 等国内用户常用软件的 MobiHok 家族样本。样本在执行过程中为了迷惑用户会安装内置的正规 APK，真正的恶意程序则隐匿执行，用户在此过程中一般感觉不到异常，从而窃取用户短信、联系人、通话记录、地理位置、键盘记录、文件目录、应用信息、手机固件信息、录音、录像、截屏、拨打电话、发送短信等。

参考链接：https://www.freebuf.com/articles/terminal/224438.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