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 30 日-2020 年 04 月 05 日　　2020 年第 14 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 431 个，其中高危漏洞 207 个、中危漏洞 184 个、低危漏洞 40 个。漏洞平均分值为 6.67。本周收录的漏洞中，涉及 0day 漏洞 151 个（占 35%），其中互联网上出现“WordPress Nashvilleparent Themes 开放重定向漏洞、Joomla! com_fabrik 目录遍历漏洞”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 3567 个，与上周（3354 个）环比增加 6%。

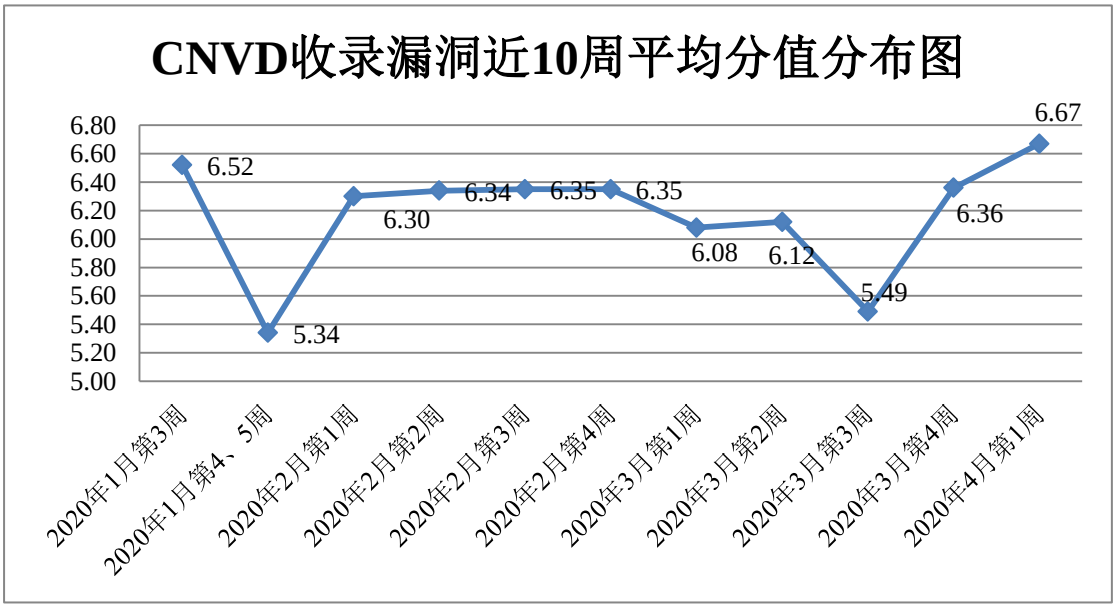

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 19 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 252 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 51 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 14 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：

北京通达信科科技有限公司、北京良精志诚科技有限责任公司、北京睿新中科教育科技有限公司、济南白菜网络技术有限公司、哈尔滨伟成科技有限公司、青岛易企天创管理咨询有限公司、北京天生创想信息技术有限公司、青岛商至信网络科技有限公司、山西牛酷信息科技有限公司、广州齐博网络科技有限公司、深圳市博思协创网络科技有限公司、北京海腾时代科技有限公司、施耐德电气公司、长沙市天心区斌网网络技术服务部、龙岩讯搜网络科技有限公司、江西大江传媒网络股份有限公司、深圳点搜科技有限公司、北京兰德华电子技术有限公司、金华市雪里开网络科技有限公司、淄博闪灵网络科技有限公司、北京康盛新创科技有限责任公司、廊坊市极致网络科技有限公司、山西先启科技有限公司、深圳市圆梦云科技有限公司、中控智慧科技股份有限公司、长沙德尚网络科技有限公司、浙江大华技术股份有限公司、上海秦王网络科技有限公司、北京理正软件股份有限公司、上海泛微网络科技股份有限公司、大连理工计算机控制工程有限公司、安徽渔之蓝教育软件技术有限公司、贵州修文农村商业银行股份有限公司、黔西花都村镇银行有限责任公司、北京亚控科技发展有限公司、三菱电机自动化（中国）有限公司、上海茸易科技有限公司、广州市九安智能技术股份有限公司、四川艾普视达数码科技有限公司、海南赞赞网络科技有限公司、微软(中国)有限公司、淄博闪灵网络科技有限公司、锐捷网络股份有限公司、安科讯（福建）科技有限公司、开平市联科网络科技有限公司、上海卓卓网络科技有限公司、南通万嘉网络科技有限公司、北京力控元通科技有限公司、拓尔思信息技术股份有限公司、铭飞科技有限公司、奕司（上海）信息科技有限公司、环保时代网、推券客联盟、廊坊市新世纪步行街畅想网络技术服务中心、微动力微信公众号管理系统、LOGA 建站系统、海洋 CMS、稻草人 cms、熊海 CMS、若依、梦雨 cms、Heybbs、PostgreSQL、Oracle Corporation、3S-Smart Software Solutions GmbH、YKCMS5、HuCart、JunAMS、FTDMS、TrueCMS、ForU CMS、OpenCart、Freecms、LOGA 和 KiteCMS。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、恒安嘉新(北京)科技股份公司、华为技术有限公司、北京神州绿盟科技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、长春嘉诚信息技术股份有限公司、北京华云安信息技术有限公司、北京铭图天成信息技术有限

公司、远江盛邦（北京）网络安全科技股份有限公司、内蒙古洞明科技有限公司、内蒙古奥创科技有限公司、河南灵创电子科技有限公司 、山石网科通信技术股份有限公司、南京众智维信息科技有限公司、杭州迪普科技股份有限公司、北京机沃科技有限公司、博智安全科技股份有限公司、北京圣博润高新技术股份有限公司、杭州海康威视数字技术股份有限公司、北京墨云科技有限公司、四川哨兵信息科技有限公司、北京长亭科技有限公司、上海观安信息技术股份有限公司、广西网信信息安全等级保护测评有限公司、吉林省吉林祥云信息技术有限公司、广州厚极信息科技有限公司、北京智游网安科技有限公司、天津市兴先道科技有限公司、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 3567 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 2468 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）	1022	1022
奇安信网神（补天平台）	963	963
上海交大	483	483
哈尔滨安天科技集团股份有限公司	258	0
北京天融信网络安全技术有限公司	243	1
恒安嘉新(北京)科技股份公司	161	0
华为技术有限公司	125	0
北京神州绿盟科技有限公司	97	21
北京启明星辰信息安全技术有限公司	84	20
新华三技术有限公司	66	0
深信服科技股份有限公司	62	0
中新网络信息安全股份有限公司	52	52
北京数字观星科技有限公司	30	0
北京奇虎科技有限公司	18	0

北京安信天行科技有限公司	9	9
北京知道创宇信息技术股份有限公司	4	1
南京联成科技发展股份有限公司	3	3
南京铱迅信息技术股份有限公司	3	3
国瑞数码零点实验室	94	94
长春嘉诚信息技术股份有限公司	71	71
北京华云安信息技术有限公司	69	69
北京铭图天成信息技术有限公司	68	68
远江盛邦（北京）网络安全科技股份有限公司	60	60
内蒙古洞明科技有限公司	52	52
内蒙古奥创科技有限公司	45	45
河南灵创电子科技有限公司	42	42
山石网科通信技术股份有限公司	33	33
南京众智维信息科技有限公司	29	29
杭州迪普科技股份有限公司	13	0
北京机沃科技有限公司	13	13
博智安全科技股份有限公司	11	11
北京圣博润高新技术股份有限公司	9	9
杭州海康威视数字技术股份有限公司	9	9
北京墨云科技有限公司	4	4
四川哨兵信息科技有限公司	4	4
北京长亭科技有限公司	3	3

上海观安信息技术股份有限公司	3	3
广西网信信息安全等级保护测评有限公司	2	2
吉林省吉林祥云信息技术有限公司	2	2
广州厚极信息科技有限公司	1	1
北京智游网安科技有限公司	1	1
天津市兴先道科技有限公司	1	1
北京浩瀚深度信息技术股份有限公司	1	1
CNCERT 广西分中心	5	5
CNCERT 安徽分中心	4	4
CNCERT 西藏分中心	4	4
CNCERT 河北分中心	2	2
CNCERT 黑龙江分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 吉林分中心	1	1
CNCERT 宁夏分中心	1	1
个人	342	342
报送总计	4685	3567

本周漏洞按类型和厂商统计

本周，CNVD 收录了 431 个漏洞。应用程序 244 个，WEB 应用 91 个，网络设备（交换机、路由器等网络端设备）55 个，操作系统 24 个，安全产品 8 个，智能设备（物联网终端设备）漏洞 6 个，数据库 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	244
WEB 应用	91

网络设备（交换机、路由器等网络端设备）	55
操作系统	24
安全产品	8
智能设备（物联网终端设备）	6
数据库	3

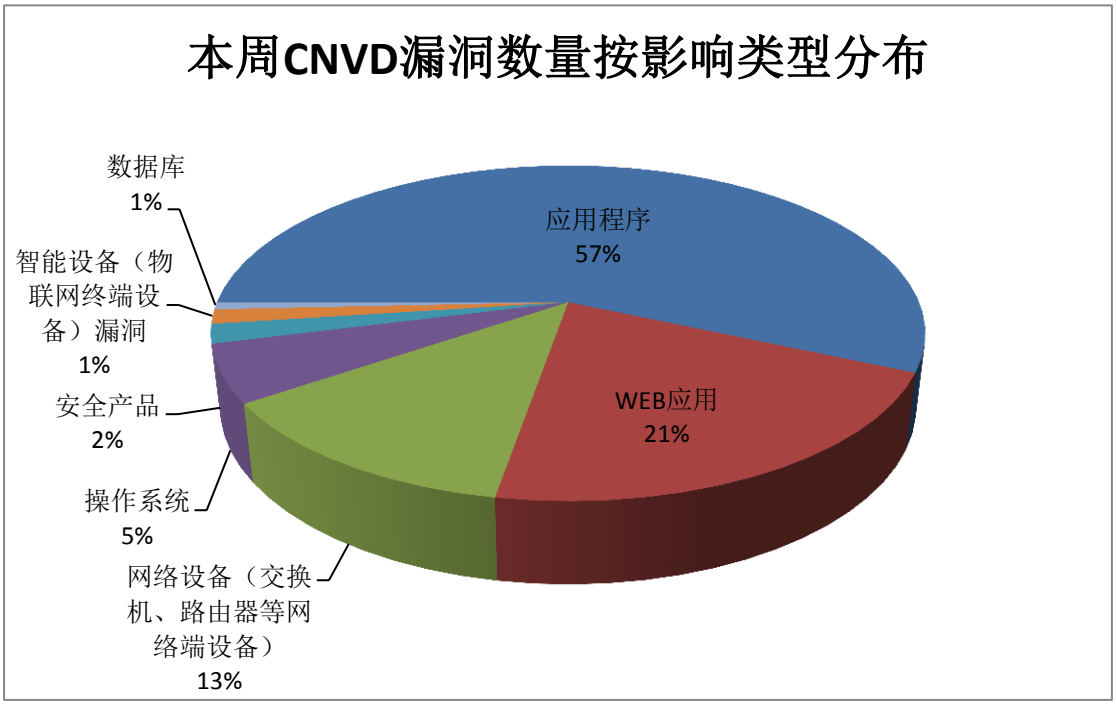

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、CloudBees、Qualcomm 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	35	8%
2	CloudBees	26	6%
3	Qualcomm	23	5%
4	IBM	13	3%
5	GitLab	12	3%
6	Quest Software	7	2%
7	Intel	7	2%
8	Joomla!	7	2%
9	Trend Micro	6	1%
10	其他	295	68%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，5 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，“Grandstream UCM6200 权限提升漏洞、MikroTik routers 资源管理错误漏洞、TCL Communication Alcatel LINKZONE 授权问题漏洞、Phoenix Contact PC WORX SRT 权限提升漏洞、KingSCADA 存在缓冲区溢出漏洞（CNVD-2020-20192）”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/

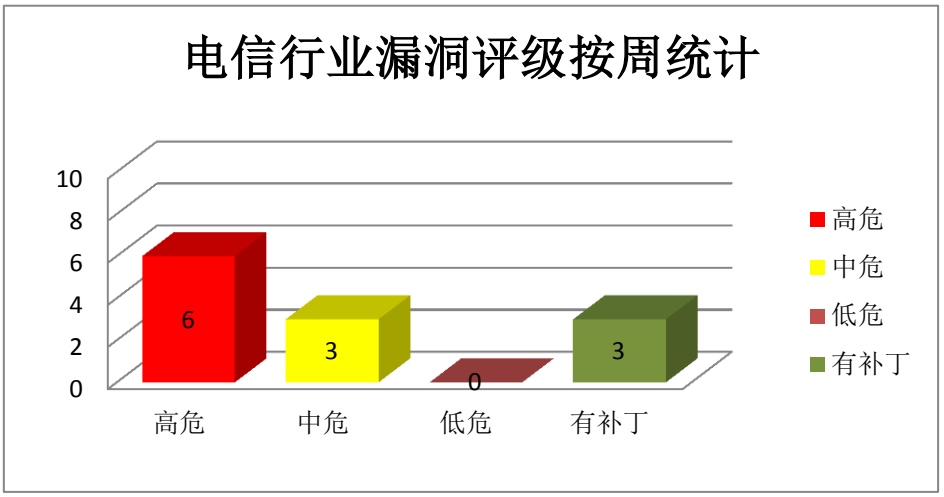

图 3 电信行业漏洞统计

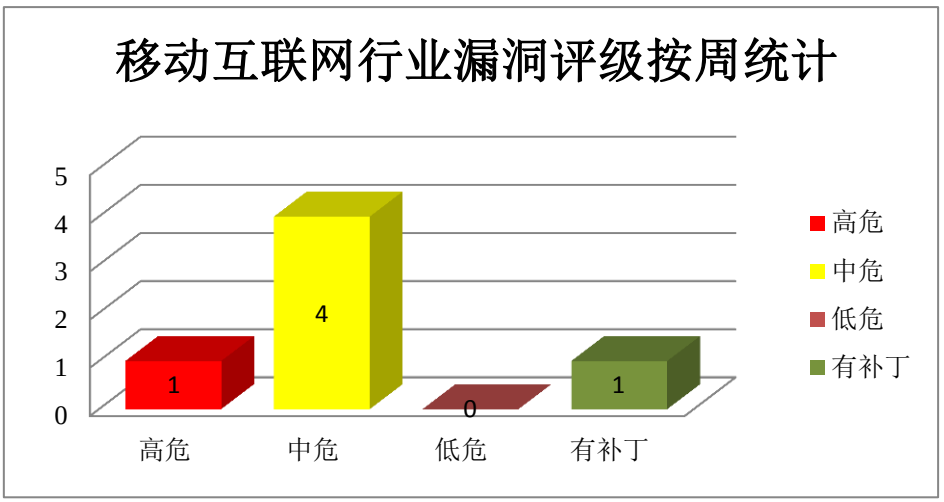

图 4 移动互联网行业漏洞统计

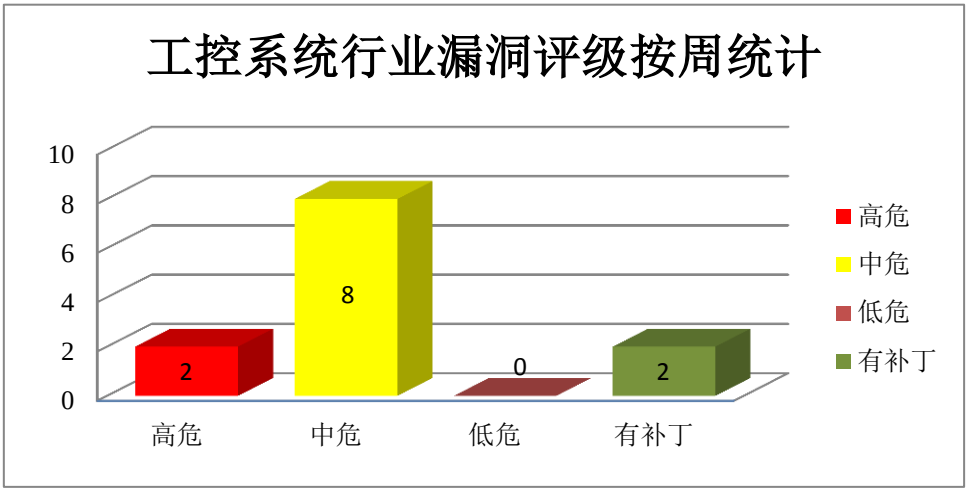

图 5 工控系统行业漏洞统计

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 ChakraCore 和 Microsoft Edge 都是美国微软（Microsoft）公司的产品。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远程代码执行漏洞，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 ChakraCore 和 Edge 远程代码执行漏洞（CNVD-2020-19965、CNVD-2020-19967、CNVD-2020-20367、CNVD-2020-20365、CNVD-2020-20368、CNVD-2020-20369、CNVD-2020-20370、CNVD-2020-20376）。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-2020-19965

https://www.cnvd.org.cn/flaw/show/CNVD-2020-19967

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20367

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20365

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20368

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20369

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20370

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20376

2、Qualcomm 产品安全漏洞

Qualcomm MDM9206 等都是美国高通（Qualcomm）公司的产品。MDM9206 是一

款中央处理器（CPU）产品。SDX24 是一款调制解调器。MSM8917 是一款中央处理器（CPU）产品。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码，导致拒绝服务和缓冲区溢出等。

CNVD 收录的相关漏洞包括：多款 Qualcomm 产品缓冲区溢出漏洞（CNVD-2020-20195、CNVD-2020-20196、CNVD-2020-20197、CNVD-2020-20202、CNVD-2020-20203）、多款 Qualcomm 产品 Data Modem 缓冲区溢出漏洞（CNVD-2020-20198、CNVD-2020-20199、CNVD-2020-20200）。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-2020-20195
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20196
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20197
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20198
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20199
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20200
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20202
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20203

3、CloudBees 产品安全漏洞

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。Splunk Plugin 是使用在其中的一个用于监控 Jenkins 主从基础架构、作业和构建过程的插件。Artifactory Plugin 是使用在其中的一个用于发布、解析和发布可跟踪的构建工件的插件。LTS 是 CloudBeesJenkins 的一个长期支持版本。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins Sandbox 认证绕过漏洞、CloudBees Jenkins Artifactory 插件信息泄露漏洞、CloudBees Jenkins 代码问题漏洞（CNVD-2020-20404、CNVD-2020-20405）、CloudBees Jenkins 信息泄露漏洞、CloudBees Jenkins 和 LTS 授权问题漏洞、CloudBees Jenkins Artifactory 插件跨站脚本漏洞、CloudBees Jenkins 跨站请求伪造漏洞（CNVD-2020-20705）。其中“CloudBees Jenkins Artifactory 插件跨站脚本漏洞”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-2020-20400
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20403
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20404
https://www.cnvd.org.cn/flaw/show/CNVD-2020-20405

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20410

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20411

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20414

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20705

4、IBM 产品安全漏洞

IBM Tivoli Netcool Impact 是美国 IBM 公司的一套网络管理软件。该软件具备自动支持关键业务功能，并提供一个可对实时的数据、事件和指示符进行统一访问的平台。IBM Spectrum Protect Plus 是一套数据保护平台。该平台为企业提供单一控制和管理点，并支持对所有规模的虚拟、物理和云环境进行备份和恢复。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命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Tivoli Netcool Impact 跨站请求伪造漏洞（CNVD-2020-20673、CNVD-2020-20675）、IBM Tivoli Netcool Impact 拒绝服务漏洞、IBM Tivoli Netcool Impact 跨站脚本漏洞（CNVD-2020-20671）、IBM Spectrum Protect Plus 命令执行漏洞（CNVD-2020-20699、CNVD-2020-20702、CNVD-2020-20698）、IBM Spectrum Protect Plus 身份验证绕过漏洞。其中，除 “IBM Tivoli Netcool Impact 拒绝服务漏洞、IBM Tivoli Netcool Impact 跨站脚本漏洞（CNVD-2020-20671）、IBM Tivoli Netcool Impact 跨站请求伪造漏”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-2020-20673

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20672

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20671

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20675

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20699

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20698

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20702

https://www.cnvd.org.cn/flaw/show/CNVD-2020-20701

5、Phoenix Contact PC WORX SRT 权限提升漏洞

Phoenix Contact PC WORX SRT 是德国菲尼克斯电气（Phoenix Contact）公司的一款可编程逻辑控制器。本周，Phoenix Contact PC WORX SRT 被披露存在权限提升漏洞。攻击者可利用该漏洞提升权限。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-2020-20687

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-2020-20386	YouPHPTube Encoder 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/YouPHPTube/YouPHPTube-Encoder/
CNVD-2020-20433	Apple macOS Catalina IOThunderboltFamily 组件资源管理错误漏洞	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.apple.com/en-us/HT211100
CNVD-2020-20437	GitLab 访问控制错误漏洞（CNVD-2020-20437）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://about.gitlab.com/2019/09/10/critical-security-release-gitlab-12-dot-2-dot-5-released/
CNVD-2020-20674	Linux kernel 信息泄露漏洞（CNVD-2020-20674）	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.kernel.org/
CNVD-2020-20678	Zoho ManageEngine Desktop Central 信息泄露漏洞（CNVD-2020-20678）	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/unauthenticated-servlet-access.html
CNVD-2020-20715	Red Hat Keycloak 信息泄露漏洞（CNVD-2020-20715）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://issues.redhat.com/browse/KEYCLOAK-12986
CNVD-2020-20724	Schneider Electric ProSoft Configurator 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.se.com/ww/en/download/document/SEVD-2020-042-01/
CNVD-2020-20731	FreeBSD 权限提升漏洞（CNVD-2020-20731）	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.freebsd.org/security/advisories/FreeBSD-SA-20:07.epair.asc
CNVD-2020-21036	Lenovo Solution Center 权限提升漏洞	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_4326
CNVD-2020-21256	Google Chrome 堆缓冲区溢出漏洞（CNVD-2020-21256）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/

小结：本周，Microsoft 产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码，破坏内存。此外 Qualcomm、CloudBees、IBM 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，执行任意代码，造成拒绝服务和缓冲区溢出等。另外，Phoenix Contact PC WORX SRT 被披露存在权限提升漏洞。攻击者可利用该漏洞提升权限。

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 Nashvilleparent Themes 开放重定向漏洞

验证描述

WordPress 是 WordPress 软件基金会的一套使用 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。

WordPress Nashvilleparent Themes 存在开放重定向漏洞。攻击者可利用漏洞成功启动仿冒欺诈和窃取用户凭据。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35206

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-20399

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. Zoom 客户端爆出安全漏洞 可向攻击者泄露 Windows 登陆凭据

作为一款音视频会议应用，Zoom 允许用户在聊天界面通过发送文本消息来互相交流。然而外媒指出，攻击者可利用聊天模块的漏洞，窃取点击了相关链接的用户的 Windows 登陆凭据。

参考链接：https://www.cnbeta.com/articles/tech/962537.htm

2. SMBGhost 漏洞允许 Windows 系统上的提权

专家发布了 Windows 上 CVE-2020-0796 权限提升漏洞的 PoC 漏洞，该漏洞被命名为 SMBGhost，可用于本地提权。不过微软表示，该漏洞已于 3 月 12 日通过带外更新进行了修补。

参考链接：https://www.securityweek.com/smbghost-vulnerability-allows-privilege-escalation-windows-systems

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