国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 05 月 18 日-2020 年 05 月 24 日　　2020 年第 21 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 289 个，其中高危漏洞 132 个、中危漏洞 136 个、低危漏洞 21 个。漏洞平均分值为 6.64。本周收录的漏洞中，涉及 0day 漏洞 122 个（占 42%），其中互联网上出现“Konica Minolta FTP Utility 'NLST'拒绝服务漏洞、Wordpress 插件 Ajax Load More '#1' SQL 注入漏洞”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 5021 个，与上周（7595 个）环比减少 34%。

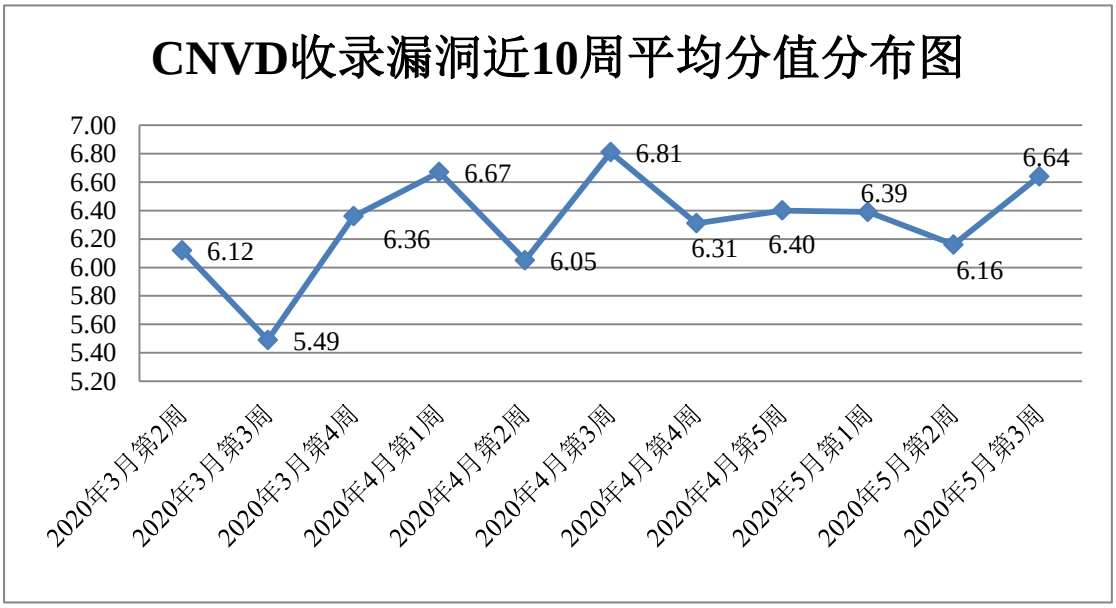

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 37 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 397 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 82 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 30 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：

北京网瑞达科技有限公司、武汉类森科技有限公司、深圳市网联信息科技开发有限公司、江西华邦传媒有限公司、中投盛世信息科技有限公司、南通万嘉网络科技有限公司、长春盘古网络技术有限公司、厦门海为科技有限公司、众联信息科技有限公司、魁网科技（重庆）有限公司、极致网络科技有限公司、山西先启科技有限公司、湖南翱云网络科技有限公司、青岛汇商传媒有限公司、北京良精志诚科技有限责任公司、淄博闪灵网络科技有限公司、西安佰联网络技术有限公司、中国联合重型燃气轮机技术有限公司、合肥天寻信息科技有限公司、大汉软件股份有限公司、茉柏枘（上海）软件科技有限公司、廊坊市极致网络科技有限公司、广州红帆电脑科技有限公司、研华科技（中国）有限公司、上海云翌通信科技有限公司、珠海金山办公软件有限公司、北京果加智能电子科技有限公司、北京翰博尔信息技术股份有限公司、西门子（中国）有限公司、锐捷网络股份有限公司、深圳市圆梦云科技有限公司、北京亚控科技发展有限公司、江西金磊科技发展有限公司、浙江标点信息科技有限公司、成都康菲顿特网络科技有限公司、深圳市锟铻科技有限公司、石家庄市征红网络科技有限公司、北京润尼尔网络科技有限公司、厦门快商通科技股份有限公司、北京致远互联软件股份有限公司、厦门科汛软件有限公司、漳州盾灵网络科技有限公司、洛阳云业信息科技有限公司、若无（上海）信息科技有限公司、上海亿速网络科技有限公司、北京七陌科技有限公司、杭州维克会网络科技有限公司、苏州烟火网络科技有限公司、海南赞赞网络科技有限公司、中建三局智能技术有限公司、中铁五局集团有限公司、景德镇铭飞科技有限公司、杭州益仕行信息技术有限公司、成都天问互联科技有限公司、施耐德电气（中国）有限公司、深圳市朗驰欣创科技有限公司、杭州恒生数字设备科技有限公司、泉州市天辉网络科技有限公司、海南易而优科技有限公司、北京五指互联科技有限公司、苏州托普斯网络科技有限公司、中文在线数字出版集团股份有限公司、开平市联科网络科技有限公司、深圳市普天宜通技术股份有限公司、盾灵科技、延边州石头网络科技服务中心、伟创互联网络技术开发团队、菏泽市定陶区子鸥网络科技服务中心、米酷影视、华晟基金、中国教育网、耳朵软件、时光设计工作室、Apache 软件基金会、苹果 CMS、逍遥 B2C 商城、海洋 CMS、梦想 CMS、大米 CMS、Heybbs、KKCMS、YCCMS、115cms 和 JunAm。

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、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、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。内蒙古奥创科技有限公司、杭州海康威视数字技术股份有限公司、山东新潮信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、国瑞数码零点实验室、上海观安信息技术股份有限公司、京东云安全、长春嘉诚信息技术股份有限公司、北京天地和兴科技有限公司、山东云天安全技术有限公司、博智安全科技股份有限公司、北京浩瀚深度信息技术股份有限公司、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、安徽长泰信息安全服务有限公司、北京华云安信息技术有限公司、北京圣博润高新技术股份有限公司及其他个人白帽子向 CNVD 提交了 5021 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 4090 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）	2554	2554
奇安信网神（补天平台）	1076	1076
阿里云计算有限公司	993	0
上海交大	460	460
哈尔滨安天科技集团股份有限公司	267	0
北京天融信网络安全技术有限公司	224	3
恒安嘉新(北京)科技股份公司	179	0
新华三技术有限公司	142	0
华为技术有限公司	126	0
深信服科技股份有限公司	86	0
北京启明星辰信息安全技术有限公司	76	0
北京神州绿盟科技有限公司	44	7
西安四叶草信息技术有限公司	39	39
中国电信集团系统集成有限责任公司	34	29

北京奇虎科技有限公司	31	10
北京数字观星科技有限公司	20	0
四川无声信息技术有限公司	15	15
杭州安恒信息技术股份有限公司	5	5
北京知道创宇信息技术股份有限公司	4	0
腾讯安全云鼎实验室	2	2
内蒙古奥创科技有限公司	237	237
杭州海康威视数字技术股份有限公司	45	45
山东新潮信息技术有限公司	45	45
远江盛邦（北京）网络安全科技股份有限公司	27	27
国瑞数码零点实验室	26	26
杭州迪普科技股份有限公司	15	0
上海观安信息技术股份有限公司	7	7
京东云安全	6	6
长春嘉诚信息技术股份有限公司	5	5
北京天地和兴科技有限公司	4	4
山东云天安全技术有限公司	4	4
博智安全科技股份有限公司	3	3
北京浩瀚深度信息技术股份有限公司	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

安徽长泰信息安全服务有限公司	1	1
北京华云安信息技术有限公司	1	1
北京圣博润高新技术股份有限公司	1	1
CNCERT 宁夏分中心	2	2
CNCERT 安徽分中心	1	1
CNCERT 广西分中心	1	1
CNCERT 河北分中心	1	1
个人	397	397
报送总计	7213	5021

本周漏洞按类型和厂商统计

本周，CNVD 收录了 289 个漏洞。应用程序 153 个，WEB 应用 84 个，网络设备（交换机、路由器等网络端设备）26 个，操作系统 14 个，数据库 6 个，安全产品 3 个，智能设备（物联网终端设备）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	153
WEB 应用	84
网络设备（交换机、路由器等网络端设备）	26
操作系统	14
数据库	6
安全产品	3
智能设备（物联网终端设备）	3

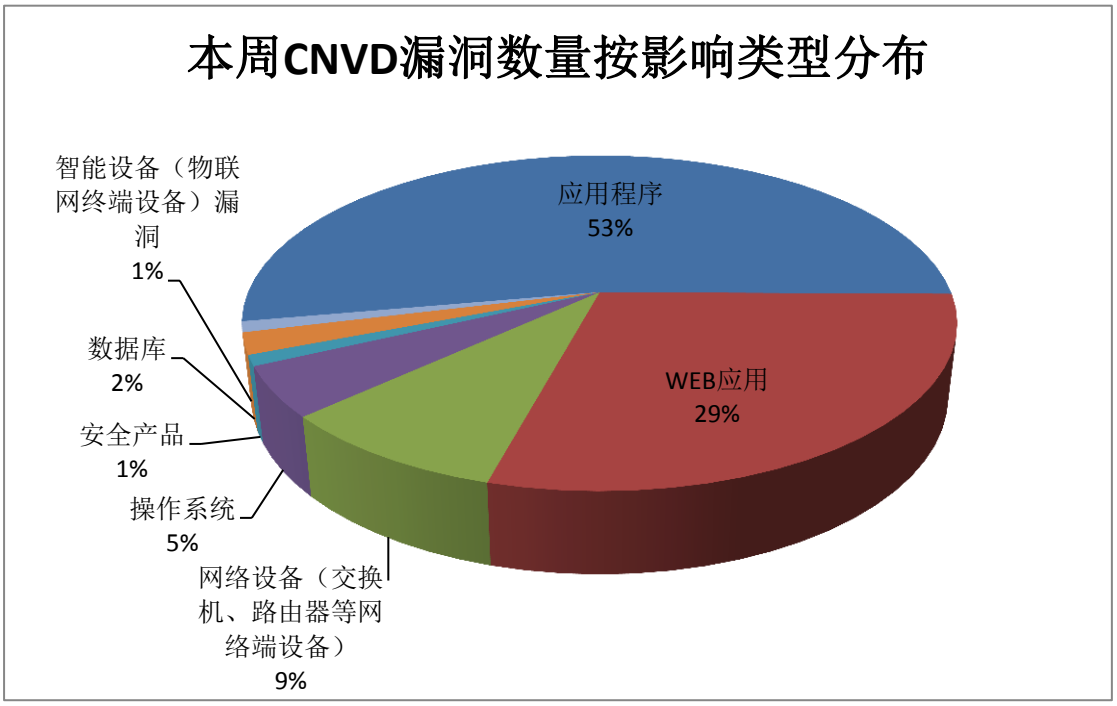

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Oracle、IBM 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	34	12%
2	Oracle	18	6%
3	IBM	17	6%
4	FreeRDP	16	6%
5	WordPress	12	4%
6	TYPO3	11	4%
7	Cisco	8	3%
8	Advantech	7	2%
9	Huawei	7	2%
10	其他	159	55%

本周行业漏洞收录情况

本周，CNVD 收录了 19 个电信行业漏洞，11 个移动互联网行业漏洞，25 个工控行业漏洞（如下图所示）。其中，“NETGEAR DGN2200 操作系统命令注入漏洞、Belden HiOS 和 HiSecOS 缓冲区溢出漏洞、ISC BIND 拒绝服务漏洞（CNVD-2020-29429）、O

pto 22 SoftPAC Project 授权问题漏洞”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/

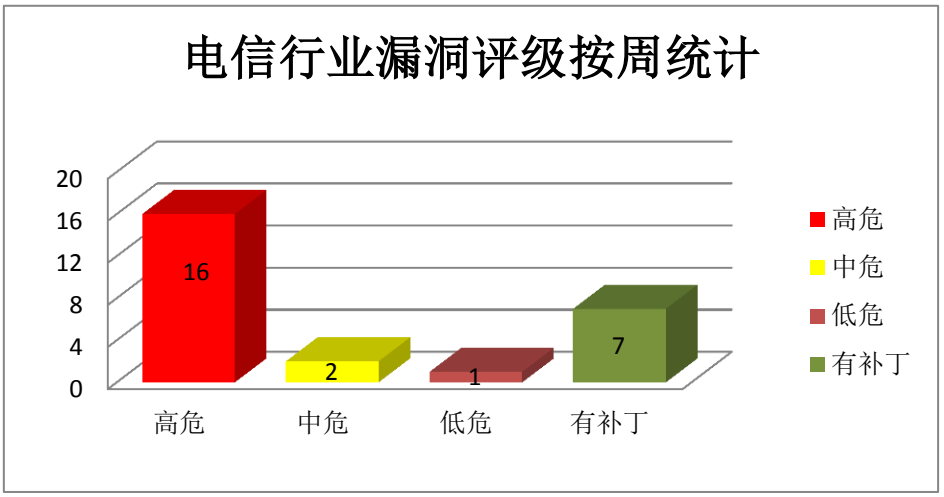

图 3 电信行业漏洞统计

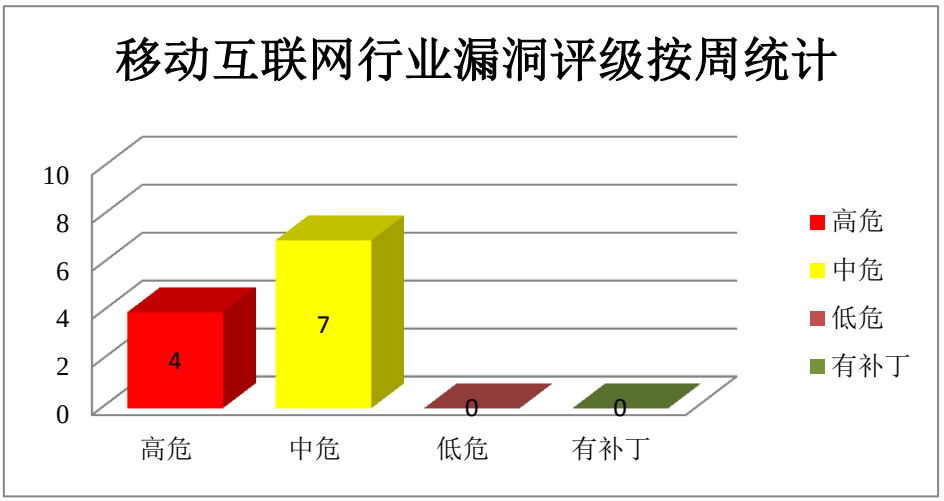

图 4 移动互联网行业漏洞统计

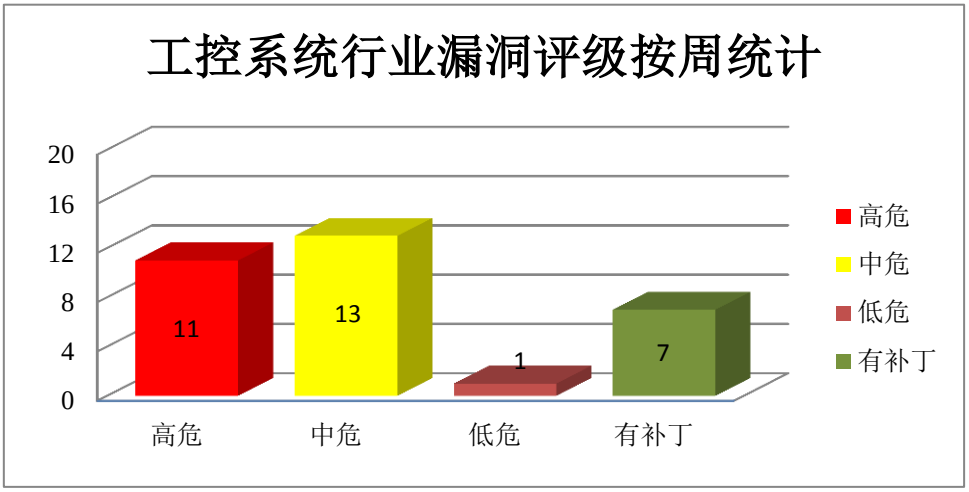

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。本周，上述产品被披露存在安全绕过漏洞，攻击者可利用漏洞绕过安全限制。

CNVD 收录的相关漏洞包括：Google Chrome 安全绕过漏洞（CNVD-2020-29226、CNVD-2020-29229、CNVD-2020-29228、CNVD-2020-29227、CNVD-2020-29232、CNVD-2020-29231、CNVD-2020-29230、CNVD-2020-29235）。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-2020-29226

https://www.cnvd.org.cn/flaw/show/CNVD-2020-29229

https://www.cnvd.org.cn/flaw/show/CNVD-2020-29228

https://www.cnvd.org.cn/flaw/show/CNVD-2020-29227

https://www.cnvd.org.cn/flaw/show/CNVD-2020-29232

https://www.cnvd.org.cn/flaw/show/CNVD-2020-29231

https://www.cnvd.org.cn/flaw/show/CNVD-2020-29230

https://www.cnvd.org.cn/flaw/show/CNVD-2020-29235

2、IBM 产品安全漏洞

IBM i2 Analysts Notebook 是一款数据可视化分析工具。该产品支持数据存储和数据分析等功能。IBM i2 Analysts Notebook Premium 是 IBM i2 Analysts Notebook 的高级版本。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞在系统上执行任意

代码，或导致应用程序崩溃（内存损坏）。

CNVD 收录的相关漏洞包括：IBM i2 Analysts Notebook 和 IBM i2 Analysts Notebook Premium 缓冲区溢出漏洞（CNVD-2020-28955、CNVD-2020-28958、CNVD-2020-28960、CNVD-2020-28964、CNVD-2020-28962、CNVD-2020-28965、CNVD-2020-29556、CNVD-2020-29555）。其中，除“IBM i2 Analysts Notebook 和 IBM i2 Analysts Notebook Premium 缓冲区溢出漏洞（CNVD-2020-29555）”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-2020-28955
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28958
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28960
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28964
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28962
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28965
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29556
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29555

3、TYPO3 产品安全漏洞

TYPO3 是一套免费开源的内容管理系统(框架)(CMS/CMF)。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数据信息，进行开放重定向，以用户权限执行脚本，导致拒绝服务等。

CNVD 收录的相关漏洞包括：TYPO3 Direct Mail 组件信息泄露漏洞（CNVD-2020-28942）、TYPO3 Backend User Interface 和 Install Tool 组件跨站脚本漏洞、TYPO3 Backend User Interface 组件代码问题漏洞、TYPO3 Core 组件代码问题漏洞、TYPO3 Direct Mail 组件输入验证错误漏洞、TYPO3 Direct Mail 组件拒绝服务漏洞、TYPO3 Password Reset 组件信息泄露漏洞、TYPO3 Direct Mail 组件信息泄露漏洞。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-2020-28942
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28944
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28945
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28947
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28949
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28951
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28950
https://www.cnvd.org.cn/flaw/show/CNVD-2020-28952

4、Cisco 产品安全漏洞

Cisco Unified Contact Center Express（Unified CCX）是一款统一通信解决方案中的客户关系管理组件。Cisco Firepower Threat Defense 是一套提供下一代防火墙服务的统一软件。Cisco Adaptive Security Appliances Software 是一套防火墙和网络安全平台。Cisco Umbrella 是一套云安全平台。Cisco Prime Collaboration Provisioning（PCP）是一套基于 Web 的下一代通信服务软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取数据库敏感信息，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Unified Contact Center Express 输入验证错误漏洞（CNVD-2020-29593）、Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 输入验证错误漏洞、Cisco Umbrella 注入漏洞、Cisco Prime Collaboration Provisioning SQL 注入漏洞（CNVD-2020-29595）、Cisco Prime Network Registrar 输入验证错误漏洞、Cisco Adaptive Security Appliances Software 和 Cisco Firepower Threat Defense 资源管理错误漏洞、Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 缓冲区溢出漏洞、Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 路径遍历漏洞。其中，除“Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 输入验证错误漏洞、Cisco Umbrella 注入漏洞、Cisco Prime Collaboration Provisioning SQL 注入漏洞（CNVD-2020-29595）”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-2020-29593
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29597
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29596
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29595
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29594
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29600
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29599
https://www.cnvd.org.cn/flaw/show/CNVD-2020-29598

5、Draytek Vigor3900、Vigor2960 和 Vigor300B 缓冲区溢出漏洞

DrayTek Vigor3900 是一款宽带路由器/VPN 网关设备。Vigor2960 是一款负载平衡路由器和 VPN 网关设备。Vigor300B 是一款负载均衡路由器。本周，Draytek Vigor3900、Vigor2960 和 Vigor300B 被披露存在缓冲区溢出漏洞。远程攻击者可借助特制 HTTP 请求利用该漏洞在系统上执行任意代码。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-2020-29583

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-2020-28763	NETGEAR DGN2200 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://kb.netgear.com/31245/DGN2200v4-Command-Execution-and-FTP-Insecure-Root-Directory-Security-Vulnerability
CNVD-2020-28765	Apache Traffic Server 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://lists.apache.org/thread.html/r21ddaf0a4a973f3c43c7ff399ae50d2f858f13f87bd6a9551c5cf6db%40%3Cannounce.trafficserver.apache.org%3E
CNVD-2020-28774	WordPress wp-google-maps 插件输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/wp-google-maps/#developers
CNVD-2020-28992	FreeRDP 缓冲区溢出漏洞（CNVD-2020-28992）	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/FreeRDP/FreeRDP/commit/17f547ae11835bb11baa3d045245dc1694866845
CNVD-2020-29315	Mozilla Thunderbird、Firefox ESR 和 Firefox 栈缓冲区溢出漏洞	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.mozilla.org/en-US/security/advisories/mfsa2020-16/
CNVD-2020-29365	Apache CloudStack 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://lists.apache.org/thread.html/rcbaafc6ae1f32e8f1e5987c243a26faf83c5172348ee7c17a54ea7f9%40%3Cusers.cloudstack.apache.org%3E
CNVD-2020-29559	Opto 22 SoftPAC Project 授权问题漏洞	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.opto22.com/
CNVD-2020-29575	Belden HiOS 和 HiSecOS 缓冲区溢出漏洞	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.belden.com/hubfs/support/security/bulletins/Belden_Security_Bulletin_BSECV-2020-01_1v2_FINAL.pdf

CNVD-2020-29586	Dell EMC Data Protection Advisor 代码注入漏洞	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/zh-cn/details/539430/DSA-2019-155-Dell-EMC-Data-Protection-Advisor-Security-Update-for-Multiple-Vulnerabilities
CNVD-2020-29585	Dell EMC Data Protection Advisor OS 命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.dell.com/support/security/zh-cn/details/539430/DSA-2019-155-Dell-EMC-Data-Protection-Advisor-Security-Update-for-Multiple-Vulnerabilities

小结：本周，Google 产品被披露存在安全绕过漏洞，攻击者可利用漏洞绕过安全限制。此外 IBM、TYPO3、Cisco 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数据信息，进行开放重定向，执行任意代码，导致拒绝服务等。另外，Draytek Vigor3900、Vigor2960 和 Vigor300B 被披露存在缓冲区溢出漏洞。远程攻击者可借助特制 HTTP 请求利用该漏洞在系统上执行任意代码。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、Konica Minolta FTP Utility 'NLST'拒绝服务漏洞

验证描述

Konica Minolta FTP Utility 是 Konica Minolta 复印机使用的一个软件。

Konica Minolta FTP Utility 'NLST'存在拒绝服务漏洞。攻击者可利用漏洞覆盖某些寄存器，例如 EAX、ESI、EDI...使 FTP 服务器崩溃并覆盖某些寄存器。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=35531

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-29213

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. ZDI 公布多个未修复的 Windows 高危 0day 详情

ZDI 安全研究人员已发布了有关微软 Windows 中五个未修补漏洞的信息，其中包括四个被认为是高风险的漏洞。

参考链接：https://www.securityweek.com/researchers-divulge-details-five-windows-zero-days

2. 蓝牙无线通信协议漏洞致无数设备易受 BIAS 攻击

以色列特拉维夫大学和以色列跨学科中心的一组研究人员发现新 DNS 漏洞，并称其为 NXNSAttack。该漏洞存在于 DNS 协议中，并且会影响所有递归 DNS 解析器，已被证实影响 NLnet Labs 的 Unbound、BIND、Knot Resolver 和 PowerDNS 等 DNS 软件，以及由谷歌、微软、Cloudflare、亚马逊、Oracle (DYN)、Verisign、IBM Quad9 和 ICANN 提供的 DNS 服务。受影响的供应商对该漏洞分别分配了 CVE 编号，包括 CVE-2020-8616(BIND)、CVE-2020-12662(Unbound)、CVE-2020-12667(Knot)、CVE-2020-10995(PowerDNS)。针对该漏洞，远程攻击者可以通过向易受攻击的解析器发送 DNS 查询来放大网络流量，该解析器会查询攻击者的权威服务器控制器。攻击者服务器将伪造的服务器名称委派给指向受害者 DNS 域的伪造服务器名，从而使解析程序生成对受害者的 DNS 服务器的查询，导致超过 1620 放大系数的 DDoS 攻击。

参考链接：https://www.securityweek.com/nxnsattack-new-dns-vulnerability-allows-big-ddos-attacks

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