国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 03 月 29 日-2021 年 04 月 04 日　　2021 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 700 个，其中高危漏洞 141 个、中危漏洞 406 个、低危漏洞 153 个。漏洞平均分值为 5.08。本周收录的漏洞中，涉及 0day 漏洞 497 个（占 71%），其中互联网上出现“Wordpress 插件 Duplicator 任意文件读取漏洞、Agentejo Cockpit 跨站脚本漏洞（CNVD-2021-24260）”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 3125 个，与上周（3128 个）环比减少 0.09%。

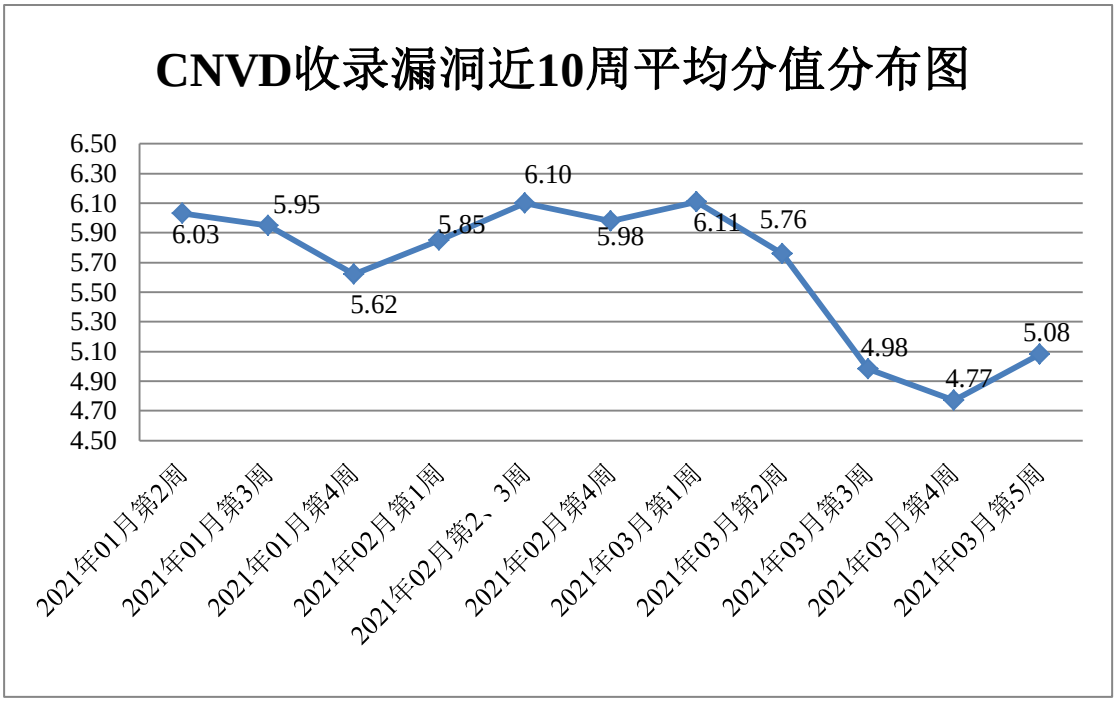

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 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 375 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 47 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 17 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：

广东凯格科技有限公司、飓风（深圳）软件有限公司、福州网钛软件科技有限公司、北京德西特科技有限公司、SUPERMICRO 科技（北京）有限公司、北京亿赛通科技发展有限责任公司、上海寰创通信科技股份有限公司、上海嵩恒网络科技股份有限公司、北京中创视讯科技有限公司、零视技术（上海）有限公司、深圳市吉祥腾达科技有限公司、上海彩圣信息科技有限公司、湖南一唯信息科技有限公司、上海焱凤信息技术有限公司、成都飞鱼星科技股份有限公司、湖北淘码千维信息科技有限公司、广州酷狗计算机科技有限公司、沈阳智虹商情广告有限公司、青岛易企天创管理咨询有限公司、任丘市正中网络科技有限公司、盘古网络集团有限公司、浙江银泰电子商务有限公司、上海互盾信息科技有限公司、上海孚盟软件有限公司、友讯电子设备（上海）有限公司、北京联高软件开发有限公司、深圳市圆梦云科技有限公司、宿迁鑫潮信息技术限公司、厦门市灵鹿谷科技有限公司、北京爱奇艺科技有限公司、江西铭软科技有限公司、上海商派网络科技有限公司、深圳市腾狐物联科技有限公司、沈阳点动科技有限公司、锐捷网络股份有限公司、廊坊市极致网络科技有限公司、深圳市磊科实业有限公司、深圳市和为顺网络技术有限公司、广州网易计算机系统有限公司、北京清大新洋科技有限公司、深圳市西迪特科技有限公司、大连华天软件有限公司、广州恒企教育科技有限公司、厦门游奕网络科技有限公司、深圳极速创想科技有限公司、北京网御星云信息技术有限公司、北京通达信科科技有限公司、深圳市永联通实业有限公司、北京致远互联软件股份有限公司、上海汉彬科技发展有限公司、太原易思软件技术有限公司、镇江市云优网络科技有限公司、长沙友点软件科技有限公司、北京盛讯美恒科技发展有限公司、迈普通信技术股份有限公司、广州市保伦电子有限公司、钉钉（中国）信息技术有限公司、苏州托普斯网络科技有限公司、上海企炬广告传媒有限公司、上海盈策信息技术有限公司、北京博乐虎科技有限公司、深圳市迅雷网络技术有限公司、海南赞赞网络科技有限公司、郑州睿智软件技术有限公司、上海溢尚网络科技有限公司、烽火通信科技股份有限公司、上海新网程信息技术股份有限公司、西安冰雪网络科技有限公司、山石网科通信技术股份有限公司、傲拓科技股份有限公司、河北鑫众博教育科技有限公司、成都今网科技有限公司、西门子（中国）有限公司、普联技术有限公司、绎览信息技术（上海）有限公司、上海梦之路数字科技有限公司、上海速擎软件有限公司、广州市九安智能技术股份有限公司、猎豹移动公司、浙江禾匠信息科技有限公司、杭州海康威视数字技术股份有限公司、深圳市天地心网络技术有限公司、合肥奇乐网络科技有限公司、北京迪科远望

科技有限公司、淄博闪灵网络科技有限公司、成都边际网络科技有限公司、河北欧润天腾云梦吧网络工作室、深圳好生意网络工作室、学并思、E 客开发团队、鱼跃 CMS、华夏 ERP、海洋 CMS、sem-cms、Zabbix、UCMS、PHPEMS、Adobe、Kanboard、PHPmyadmin、Heybbs 和 HDHCMS。

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、阿里云计算有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。北京信联科汇科技有限公司、江苏保旺达软件技术有限公司、南京众智维信息科技有限公司、北京山石网科信息技术有限公司、北京华云安信息技术有限公司、河南灵创电子科技有限公司、博智安全科技股份有限公司、河南信安世纪科技有限公司、北京天地和兴科技有限公司、山东泽鹿安全技术有限公司（泽鹿安全）、任子行网络技术股份有限公司、山东云天安全技术有限公司、山东新潮信息技术有限公司、杭州海康威视数字技术股份有限公司、浙江御安信息技术有限公司、上海纽盾科技股份有限公司、山东华鲁科技发展股份有限公司、北京安帝科技有限公司、京东云安全、四川哨兵信息科技有限公司、武汉明嘉信信息安全检测评估有限公司、贵州多彩宝互联网服务有限公司、广州安亿信软件科技有限公司、山石网科通信技术股份有限公司、杭州木链物联网科技有限公司、工业信息安全（四川）创新中心有限公司、长春嘉诚信息技术股份有限公司、北方实验室（沈阳）股份有限公司、北京远禾科技有限公司、上海观安信息技术股份有限公司、北京君云天下科技有限公司、中国通信服务重庆公司（安知攻防实验室）、上海崤函信息科技有限公司、重庆贝特计算机系统工程有限公司、海南神州希望网路有限公司、上海蜚语信息科技有限公司、西安交通大学及其他个人白帽子向 CNVD 提交了 3125 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、奇安信网神（补天平台）和上海交大向 CNVD 共享的白帽子报送的 1737 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）	957	957
奇安信网神（补天平台）	395	395
上海交大	385	385
哈尔滨安天科技集团股份有限公司	321	0
阿里云计算有限公司	245	0
北京神州绿盟科技有限公司	136	9

深信服科技股份有限公司	101	1
北京天融信网络安全技术有限公司	97	3
北京数字观星科技有限公司	92	0
华为技术有限公司	80	0
新华三技术有限公司	63	0
北京启明星辰信息安全技术有限公司	61	0
中国电信股份有限公司网络安全产品运营中心	32	22
恒安嘉新（北京）科技股份公司	31	0
北京奇虎科技有限公司	30	30
天津市国瑞数码安全系统股份有限公司（国瑞数码零点实验室）	19	19
远江盛邦（北京）网络安全科技股份有限公司	3	3
北京知道创宇信息技术股份有限公司	1	0
内蒙古奥创科技有限公司	1	1
北京信联科汇科技有限公司	177	177
江苏保旺达软件技术有限公司	56	56
南京众智维信息科技有限公司	47	47
北京山石网科信息技术有限公司	43	43
北京华云安信息技术有限公司	36	36
河南灵创电子科技有限公司	32	32
杭州迪普科技股份有限公司	30	0
博智安全科技股份有	27	27

限公司		
河南信安世纪科技有限公司	24	24
北京天地和兴科技有限公司	20	20
山东泽鹿安全技术有限公司（泽鹿安全）	19	19
任子行网络技术股份有限公司	15	15
山东云天安全技术有限公司	15	15
山东新潮信息技术有限公司	14	14
杭州海康威视数字技术股份有限公司	14	14
浙江御安信息技术有限公司	14	14
上海纽盾科技股份有限公司	10	10
山东华鲁科技发展股份有限公司	9	9
北京安帝科技有限公司	6	6
京东云安全	6	6
四川哨兵信息科技有限公司	5	5
武汉明嘉信信息安全检测评估有限公司	5	5
贵州多彩宝互联网服务有限公司	4	4
广州安亿信软件科技有限公司	4	4
山石网科通信技术股份有限公司	3	3
杭州木链物联网科技有限公司	3	3
工业信息安全（四川）创新中心有限公司	2	2
长春嘉诚信息技术股份有限公司	2	2
北方实验室（沈阳）股份有限公司	2	2
北京远禾科技有限公	2	2

司		
上海观安信息技术股份有限公司	1	1
北京君云天下科技有限公司	1	1
中国通信服务重庆公司（安知攻防实验室）	1	1
上海崤函信息科技有限公司	1	1
重庆贝特计算机系统工程有限公司	1	1
海南神州希望网路有限公司	1	1
上海蜚语信息科技有限公司	1	1
西安交通大学	1	1
CNCERT 西藏分中心	6	6
CNCERT 浙江分中心	3	3
CNCERT 贵州分中心	1	1
CNCERT 山东分中心	1	1
个人	665	665
报送总计	4380	3125

本周漏洞按类型和厂商统计

本周，CNVD 收录了 700 个漏洞。应用程序 322 个，WEB 应用 251 个，操作系统 48 个，网络设备（交换机、路由器等网络端设备）36 个，安全产品 28 个，智能设备（物联网终端设备）15 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	322
WEB 应用	251
操作系统	48
网络设备（交换机、路由器等网络端设备）	36
安全产品	28
智能设备（物联网终端设备）	15

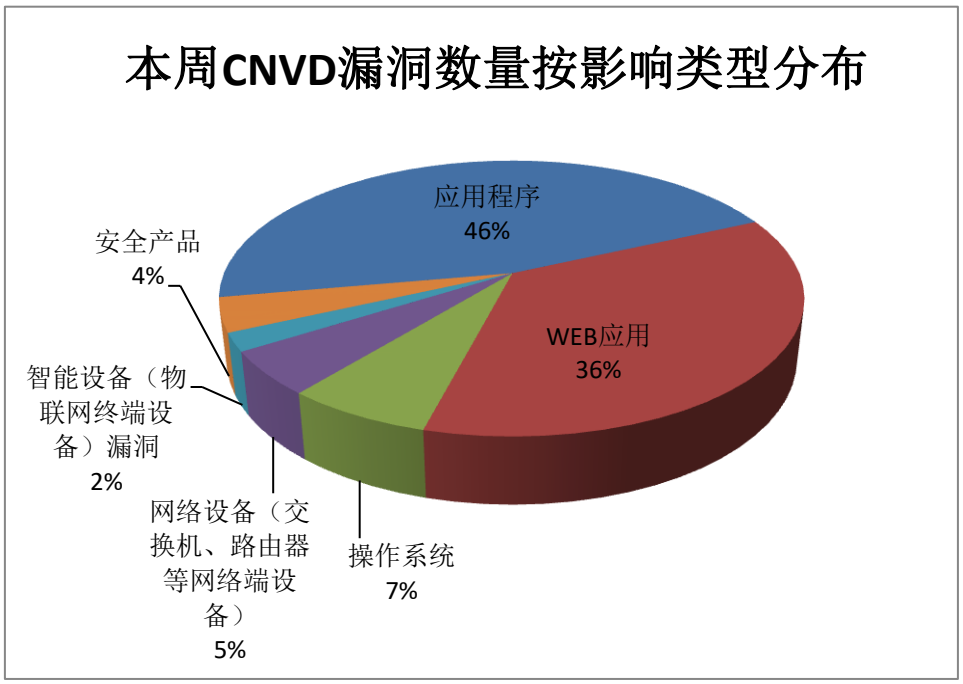

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及北京海腾时代科技有限公司、Microsoft、Huawei 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	北京海腾时代科技有限公司	56	8%
2	Microsoft	50	7%
3	Huawei	20	3%
4	Cisco	15	2%
5	新华三技术有限公司	14	2%
6	Google	13	2%
7	研华科技（中国）有限公司	11	2%
8	VMware	10	1%
9	WordPress	10	1%
10	其他	501	72%

本周行业漏洞收录情况

本周，CNVD 收录了 45 个电信行业漏洞，31 个移动互联网行业漏洞，24 个工控行业漏洞（如下图所示）。其中，“Google Android Framework 权限提升漏洞（CNVD-2021-22971、CNVD-2021-22973、CNVD-2021-22974）”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/

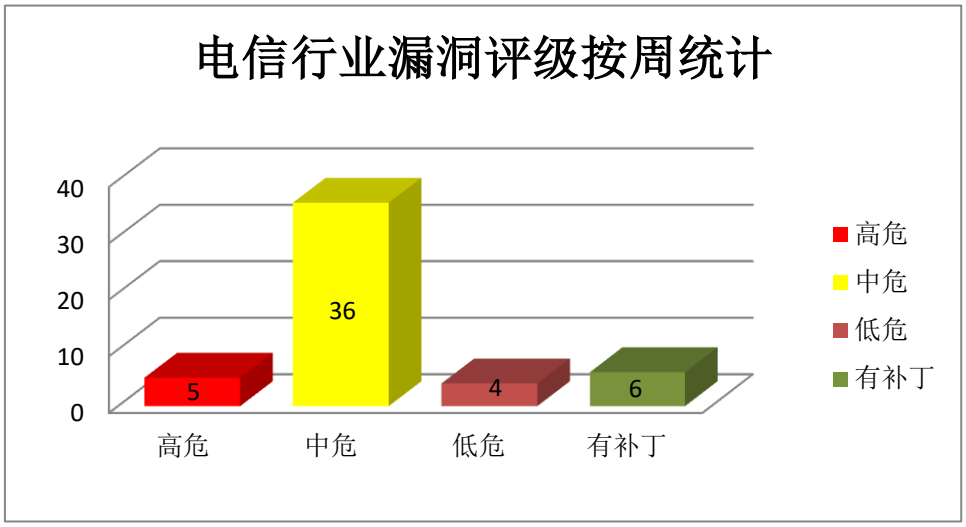

图 3 电信行业漏洞统计

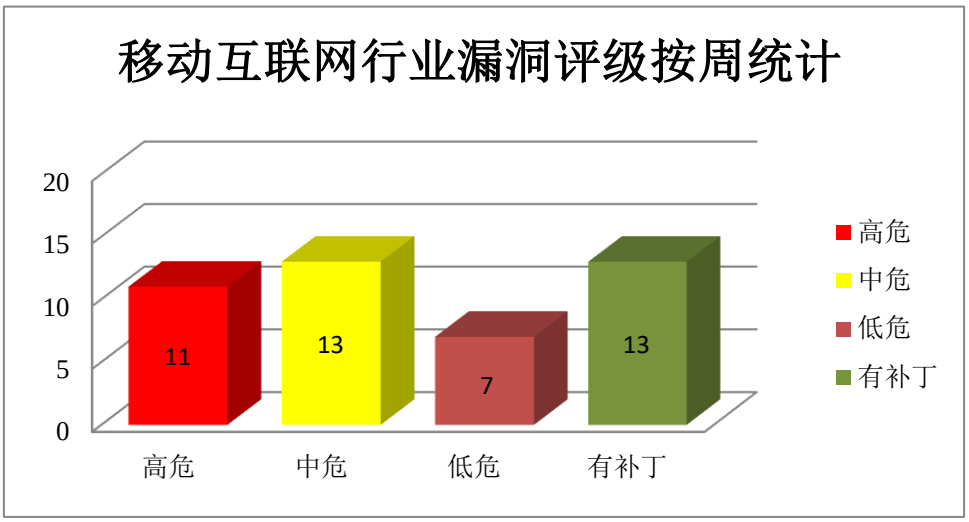

图 4 移动互联网行业漏洞统计

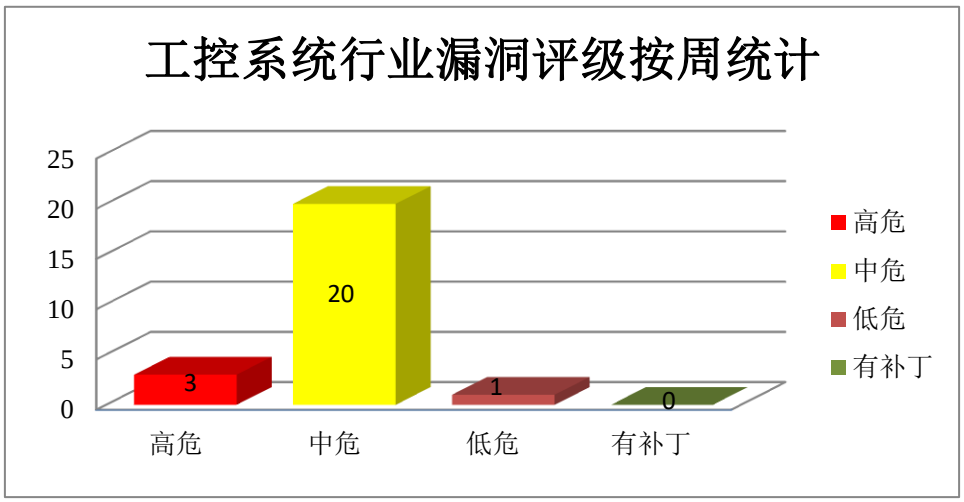

图 5 工控系统行业漏洞统计

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 Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。VBScript Engine 是其中的一个 VBScript 脚本语言引擎。Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码，导致内存损坏。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer VBScript Engine 远程代码执行漏洞（CNVD-2021-24004、CNVD-2021-24003、CNVD-2021-24002、CNVD-2021-24007、CNVD-2021-24006、CNVD-2021-24005）、Microsoft Excel 远程代码执行漏洞（CNVD-2021-24042、CNVD-2021-24041）。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-2021-24004
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24003
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24002
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24007
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24006
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24005
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24042
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24041

2、Cisco 产品安全漏洞

Cisco Jabber 是一个网络会议和即时消息传递应用程序，允许用户通过可扩展消息传递和状态协议（XMPP）发送消息。Cisco IOS XE 是美国 Cisco 公司为其网络设备开发的一套基于 Linux 内核的模块化操作系统。Cisco Iox 是美国思科（Cisco）公司的一个结合了 Cisco IOS 和 Linux OS 用于安全网络连接以及开发 IOT 应用的安全开发环境。Cisco Identity Services Engine (ISE)是下一代身份和访问控制策略平台，使企业能够执行合规性、增强基础架构安全性并简化其服务操作。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞收集有关系统配置的敏感信息，覆盖驻留在底层主机文件系统上的任意文件，以 root 用户身份执行任意命令等。

CNVD 收录的相关漏洞包括：Cisco Jabber 信息泄露漏洞（CNVD-2021-22911）、C

isco IOS XE 命令注入漏洞（CNVD-2021-22914、CNVD-2021-24467）、Cisco IOx Application 拒绝服务漏洞、Cisco Jabber 代码执行漏洞、Cisco IOS XE 任意文件覆盖漏洞（CNVD-2021-24468）、Cisco Identity Services Engine 信息泄露漏洞（CNVD-2021-24476、CNVD-2021-24475）。其中“Cisco Jabber 信息泄露漏洞（CNVD-2021-22911）、Cisco Jabber 代码执行漏洞、Cisco IOS XE 命令注入漏洞（CNVD-2021-24467）”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-2021-22911
https://www.cnvd.org.cn/flaw/show/CNVD-2021-22914
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24462
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24466
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24468
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24467
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24476
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24475

3、Huawei 产品安全漏洞

Huawei P30 是中国华为（Huawei）公司的一款智能手机。Huawei NGFW Module 是一款下一代防火墙（NGFW）模块。Huawei NIP6800 是一套入侵防御系统。Huawei NIP6300 是一款主要适用于企业、学校、运行商、IDC 的入侵防御系统。Huawei USG6600 是一款数据中防火墙产品。Secospace USG6600 是一款下一代防火墙产品。Huawei S2700 是一款企业级交换机产品。Huawei USG9500 是一款数据中心防火墙产品。Huawei USG9520 是一款应用于大型环境的防火墙设备。Huawei USG9560 是一款应用于大型环境的防火墙设备。Huawei eUDC660 是中国华为（Huawei）公司的一款用于提供调度功能的设备。Huawei Manageone 是中国华为（Huawei）公司的一套云数据中心管理解决方案。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，以不合理权限执行某些操作，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei P30 内存写漏洞、多款 Huawei 产品拒绝服务漏洞（CNVD-2021-24915、CNVD-2021-24914）、多款 Huawei 产品 UAF 漏洞、Huawei USG9500 信息泄露漏洞（CNVD-2021-24917）、多款 Huawei 产品信息泄露漏洞（CNVD-2021-24916）、Huawei eUDC660 不适当资源管理漏洞、Huawei ManageOne 权限分配不当漏洞。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-2021-24911
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24915
https://www.cnvd.org.cn/flaw/show/CNVD-2021-24914

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24913

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24917

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24916

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24920

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24918

4、Google 产品安全漏洞

Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，导致权限提升。

CNVD 收录的相关漏洞包括：Google Android Framework 权限提升漏洞（CNVD-2021-22972、CNVD-2021-22971、CNVD-2021-22974、CNVD-2021-22973）、Google Android 权限提升漏洞（CNVD-2021-24922、CNVD-2021-24924、CNVD-2021-24923）、Google Android 信息泄露漏洞（CNVD-2021-24921）。其中，“Google Android Framework 权限提升漏洞（CNVD-2021-22971、CNVD-2021-22974、CNVD-2021-22973）”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-2021-22972

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22971

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22974

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22973

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24922

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24921

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24924

https://www.cnvd.org.cn/flaw/show/CNVD-2021-24923

5、Linux kernel 拒绝服务漏洞（CNVD-2021-24347）

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。本周，Linux kernel 被披露存在拒绝服务漏洞。攻击者可利用漏洞造成系统崩溃。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-2021-24347

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-2021-22910	Cisco Jabber 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.webex.com/downloads/jabber.html
CNVD-2021-22920	Microsoft Windows Kernel 权限提升漏洞（CNVD-2021-22920）	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-2020-1266
CNVD-2021-22955	Invigo Automatic Device Management 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.on-x.com/sites/default/files/security_advisory_-_multiple_vulnerabilities_-_invigo_adm.pdf
CNVD-2021-23790	BaserCMS OS 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://basercms.net/security/JVN64869876
CNVD-2021-24024	GE MU320E 硬编码密码漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.gegridsolutions.com/Passport/Login.aspx?ReturnUrl=%2fapp%2fviewfiles.aspx%3fprod%3dMU320E%26type%3d21
CNVD-2021-24029	Raw Image Extension 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17086
CNVD-2021-24268	UPX 拒绝服务漏洞（CNVD-2021-24268）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/upx/upx/commit/3781df9da23840e596d5e9e8493f22666802fe6c
CNVD-2021-24267	GNU libmicrohttpd 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://bugzilla.redhat.com/show_bug.cgi?id=1939127
CNVD-2021-24277	Centreon 远程代码执行漏洞（CNVD-2021-24277）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/centreon/centreon/pull/8467
CNVD-2021-24274	MarkAny MaEPSBroker 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://www.markany.com/eng/

小结：本周，Microsoft 产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在当

前用户的上下文中执行任意代码，导致内存损坏。此外，Cisco、Huawei、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞收集有关系统配置的敏感信息，覆盖驻留在底层主机文件系统上的任意文件，以 root 用户身份执行任意命令，导致拒绝服务等。另外，Linux kernel 被披露存在拒绝服务漏洞。攻击者可利用漏洞造成系统崩溃。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 插件 Duplicator 任意文件读取漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

Wordpress 插件 Duplicator 存在任意文件读取漏洞。攻击者可利用漏洞以 web 服务器权限读取任意文件。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2020120128

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-24910

信息提供者

深信服科技股份有限公司

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. Ovarro TBox RTU 的漏洞可能会使工业系统遭受远程攻击

Ovarro 的 TBox 远程终端单元（RTU）中发现了多达五个漏洞，如果不进行修补，可能会为不断升级的针对关键基础设施的攻击打开大门，例如远程代码执行和拒绝服务。

参考链接：https://thehackernews.com/2021/03/flaws-in-ovarro-tbox-rtus-could-open.html

2. 新的漏洞可能使黑客绕过 Linux 系统上的 Spectre 攻击缓解措施

网络安全研究人员披露了基于 Linux 的操作系统中的两个新漏洞，如果成功利用这些漏洞，攻击者可以规避缓解诸如 Spectre 之类的推测性攻击的方法，并从内核内存中获取敏感信息。

参考链接：https://thehackernews.com/2021/03/new-bugs-could-let-hackers-bypass.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