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 22 日-2021 年 03 月 28 日　　2021 年第 12 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 719 个，其中高危漏洞 166 个、中危漏洞 249 个、低危漏洞 304 个。漏洞平均分值为 4.77。本周收录的漏洞中，涉及 0day 漏洞 507 个（占 71%），其中互联网上出现“Froala WYSIWYG HTML Editor 跨站脚本漏洞、GoodLayers LMS for Wordpress 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 3128 个，与上周（4981 个）环比减少 37%。

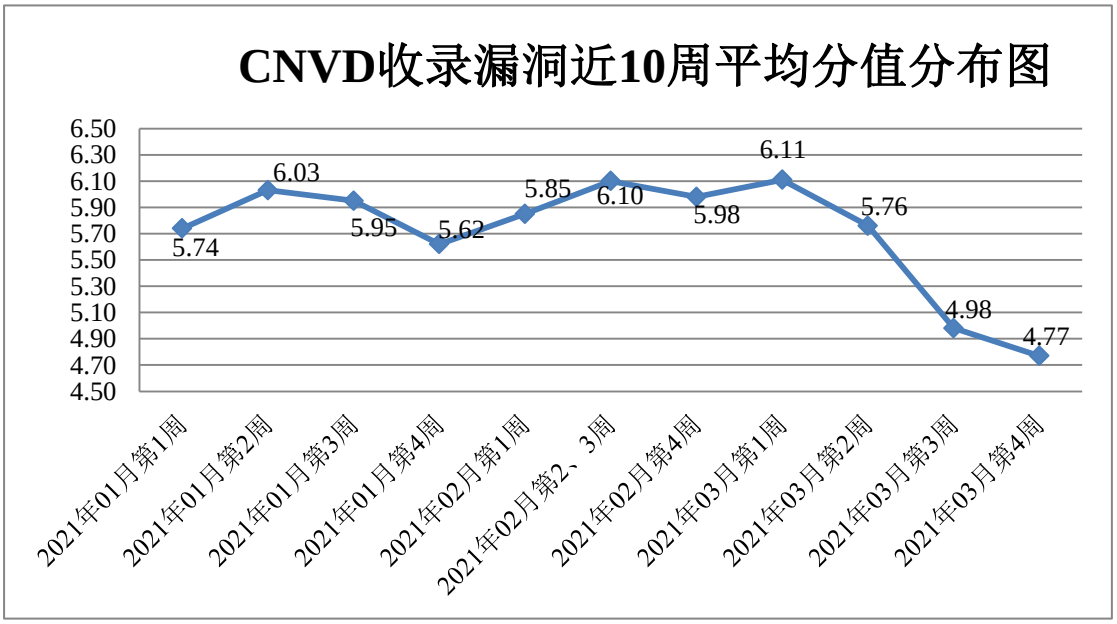

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向基础电信企业通报漏洞事件 8 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 413 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 46 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 26 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：

北京派网软件有限公司、杭州萤石科技有限公司、美图公司、淄博闪灵网络科技有限公司、哈尔滨伟成科技有限公司、杭州品茗信息技术有限公司、杭州海康威视数字技术股份有限公司、普联技术有限公司、深圳维盟科技股份有限公司、深圳市捷顺科技实业股份有限公司、上海泛微网络科技股份有限公司、北京网易有道计算机系统有限公司、杭州冠航科技有限公司、深圳市磊科实业有限公司、北京网御星云信息技术有限公司、海居亦科技发展有限公司、深圳极速创想科技有限公司、北京中创视讯科技有限公司、友讯电子设备（上海）有限公司、北京清大新洋科技有限公司、南昌云端网络科技有限公司、上海牛迈网络科技有限公司、深圳市邦明科技有限公司、深圳市英威腾电气股份有限公司、广州市九安智能技术股份有限公司、广州红帆科技有限公司、厦门科拓通讯技术股份有限公司、成都生动网络科技有限公司、武汉金同方科技有限公司、锐捷网络股份有限公司、北京京宽科技发展有限公司、中电华通通信有限公司北京分公司、润迅数据集团有限公司、雷神（武汉）信息技术有限公司、北京亚控科技发展有限公司、北京东方通科技股份有限公司、四平市九州易通科技有限公司、海别得（上海）商贸有限公司、厦门市南希网络科技有限公司、武汉沃讯科技有限公司、北京中睿天下信息技术有限公司、中兴通讯股份有限公司、苏州祥云平台信息技术有限公司、河南方果电子科技有限公司、四创科技有限公司、上海二三四五移动科技有限公司、新东方教育科技集团有限公司、南通协达软件有限公司、北京良精志诚科技有限责任公司、北京飞书科技有限公司、天信仪表集团有限公司、北京格林伟迪科技股份有限公司、成都市大任软件有限责任公司、研华科技（中国）有限公司、上海穆云智能科技有限公司、苏州烟火网络科技有限公司、广东凯格科技有限公司、深圳市因纳特科技有限公司、北京一诺互联科技有限公司、西安新软信息科技有限公司、杭州盈高科技有限公司、上海艾泰科技有限公司、上海宁盾信息科技有限公司、哈尔滨奇讯科技有限公司、深圳市吉祥腾达科技有限公司、广州津虹网络传媒有限公司、合肥晨光电子科技有限公司、上海金慧软件有限公司、北京新东方迅程网络科技股份有限公司、宿迁市乐创信息科技有限公司、杭州阔知网络科技有限公司、国晋信息科技有限公司、深圳零壹信息科技有限责任公司、万兴科技集团股份有限公司、江苏欧索软件有限公司、北京天润顺腾科技有限公司、傲拓科技股份有限公司、上海甄云信息科技有限公司、安徽希望网络科技有限公司、南京先极科技有限公司、深圳市天地心网络技术有限公司、北京力控元通科技有限公司、常熟市祺迹网络信息科技有限公司、唐山平升电子技术开发有限公司、北京百家互联科技有限公司、大唐电信科技股份有限公司、成都飞鱼星科技股份有限公司、纬衡浩建科技（深圳）有限公司、廊坊市极致网络科技有限公司、北京碧海威科技有限公司、太原迅易科

技有限公司、宁波市鄞州天一科技有限公司、上海博达数据通信有限公司、联想集团、河北欧润天腾云梦吧网络工作室、鑫运网络、睿谷信息、京东安全应急响应中心、方正集团、环保时代网、华夏 ERP、wmcms 团队、快排 CMS、PHPEMS、sem-cms、XDcms、ShuipFCMS 、ke361、GeeLeaf 、A3MALL 、SEMCMS、Microsoft、The Apache Software Foundation、MessageSolution 、DiYunCMS 和 bento4。

本周，CNVD 发布了《Microsoft 发布 2021 年 3 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6221

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、华为技术有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。北京华云安信息技术有限公司、北京信联科汇科技有限公司、南京众智维信息科技有限公司、山东新潮信息技术有限公司、河南信安世纪科技有限公司、北京山石网科信息技术有限公司、北京天地和兴科技有限公司、江苏保旺达软件技术有限公司、河南灵创电子科技有限公司、山东华鲁科技发展股份有限公司、西安交大捷普网络科技有限公司、北京顶象技术有限公司、山东云天安全技术有限公司、武汉明嘉信信息安全检测评估有限公司、北京安帝科技有限公司、博智安全科技股份有限公司、杭州迪普科技股份有限公司、北京华顺信安科技有限公司、木链科技、长春嘉诚信息技术股份有限公司、京东云安全、浙江御安信息技术有限公司、福建省海峡信息技术有限公司、山石网科通信技术股份有限公司、上海纽盾科技股份有限公司、四川哨兵信息科技有限公司、上海观安信息技术股份有限公司、浙江乾冠信息安全研究院、贵州多彩宝互联网服务有限公司、工业信息安全（四川）创新中心有限公司、上海嵴函信息科技有限公司、北京创安恒宇科技有限公司、腾讯安全天马实验室、北京君云天下科技有限公司及其他个人白帽子向 CNVD 提交了 3128 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 1506 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）	1083	1083
哈尔滨安天科技集团股份有限公司	326	0
北京天融信网络安全技术有限公司	249	3

奇安信网神（补天平台）	229	229
上海交大	194	194
华为技术有限公司	142	0
北京神州绿盟科技有限公司	136	2
北京数字观星科技有限公司	116	0
新华三技术有限公司	97	0
远江盛邦（北京）网络安全科技股份有限公司	81	81
中国电信股份有限公司网络安全产品运营中心	65	45
深信服科技股份有限公司	61	1
北京启明星辰信息安全技术有限公司	53	1
卫士通信息产业股份有限公司	51	0
北京奇虎科技有限公司	32	32
西安四叶草信息技术有限公司	26	26
中国电信集团系统集成有限责任公司	24	24
恒安嘉新（北京）科技股份公司	11	0
北京安信天行科技有限公司	8	8
天津市国瑞数码安全系统股份有限公司	7	7
内蒙古奥创科技有限	5	5

公司		
北京知道创宇信息技术股份有限公司	2	0
北京智游网安科技有限公司	1	1
北京华云安信息技术有限公司	128	128
北京信联科汇科技有限公司	98	98
南京众智维信息科技有限公司	83	83
山东新潮信息技术有限公司	46	46
河南信安世纪科技有限公司	36	36
北京山石网科信息技术有限公司	35	35
北京天地和兴科技有限公司	31	31
江苏保旺达软件技术有限公司	30	30
河南灵创电子科技有限公司	30	30
山东华鲁科技发展股份有限公司	20	20
西安交大捷普网络科技有限公司	20	20
北京顶象技术有限公司	18	18
山东云天安全技术有限公司	17	17
武汉明嘉信信息安全检测评估有限公司	15	15
北京安帝科技有限公	14	14

司		
博智安全科技股份有限公司	10	10
杭州迪普科技股份有限公司	9	0
北京华顺信安科技有限公司	8	0
木链科技	6	6
长春嘉诚信息技术股份有限公司	5	5
京东云安全	5	5
浙江御安信息技术有限公司	5	5
福建省海峡信息技术有限公司	4	4
山石网科通信技术股份有限公司	3	3
上海纽盾科技股份有限公司	3	3
四川哨兵信息科技有限公司	2	2
上海观安信息技术股份有限公司	2	2
浙江乾冠信息安全研究院	2	2
贵州多彩宝互联网服务有限公司	2	2
工业信息安全（四川）创新中心有限公司	1	1
上海峭函信息科技有限公司	1	1
北京创安恒宇科技有限公司	1	1
腾讯安全天马实验室	1	1

北京君云天下科技有限公司	1	1
CNCERT 西藏分中心	12	12
CNCERT 宁夏分中心	16	16
CNCERT 贵州分中心	4	4
CNCERT 浙江分中心	1	1
个人	678	678
报送总计	4402	3128

本周漏洞按类型和厂商统计

本周，CNVD 收录了 719 个漏洞。应用程序 410 个，WEB 应用 177 个，操作系统 58 个，网络设备（交换机、路由器等网络端设备）37 个，智能设备（物联网终端设备）27 个，安全产品 9 个，数据库 1 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	410
WEB 应用	177
操作系统	58
网络设备（交换机、路由器等网络端设备）	37
智能设备（物联网终端设备）漏洞	27
安全产品	9
数据库	1

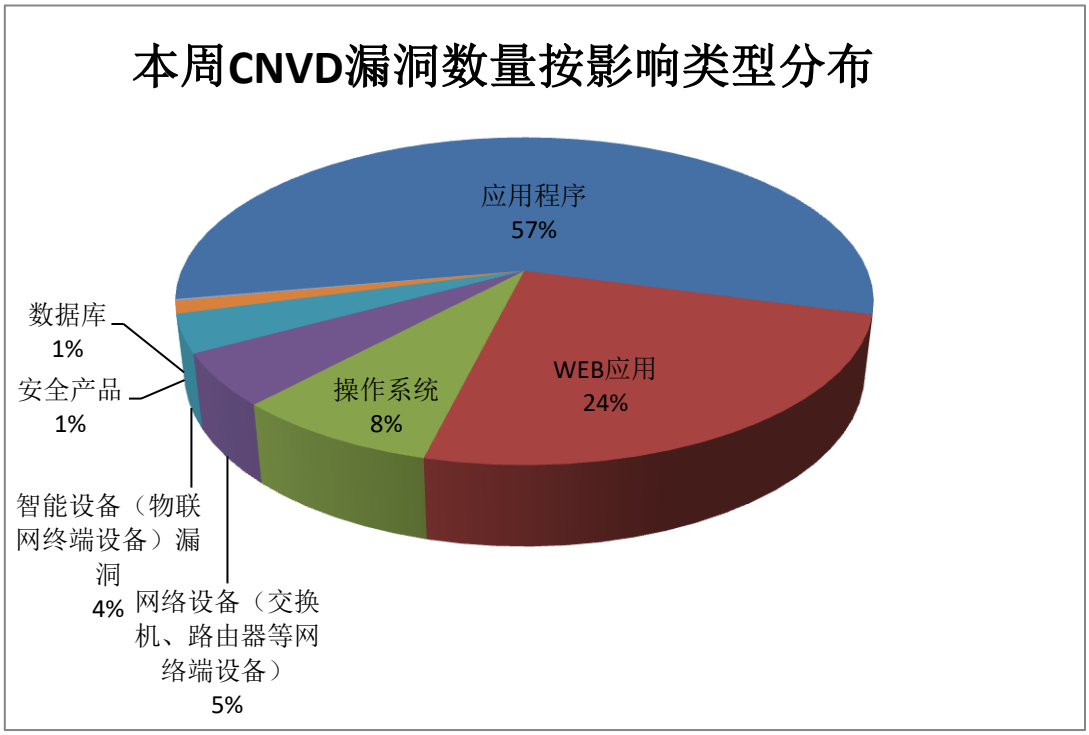

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及深圳市腾讯计算机系统有限公司、江下信息科技（惠州）有限公司、Cisco 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	深圳市腾讯计算机系统有限公司	46	7%
2	江下信息科技（惠州）有限公司	30	4%
3	Cisco	19	3%
4	Schneider Electric	15	2%
5	Linux	14	2%
6	Palo Alto Networks	11	2%
7	Google	10	1%
8	新华三技术有限公司	10	1%
9	WordPress	9	1%
10	其他	555	77%

本周行业漏洞收录情况

本周，CNVD 收录了 46 个电信行业漏洞，37 个移动互联网行业漏洞，20 个工控行业漏洞（如下图所示）。其中，“Cisco IOS XE 拒绝服务漏洞（CNVD-2021-22166）、D-Link DIR-825 缓冲区溢出漏洞、Google Android Framework 权限提升漏洞（CNVD-202

1-19754）、Baxter ExactaMix EM2400 和 ExactaMix EM1200 信任管理问题漏洞”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/

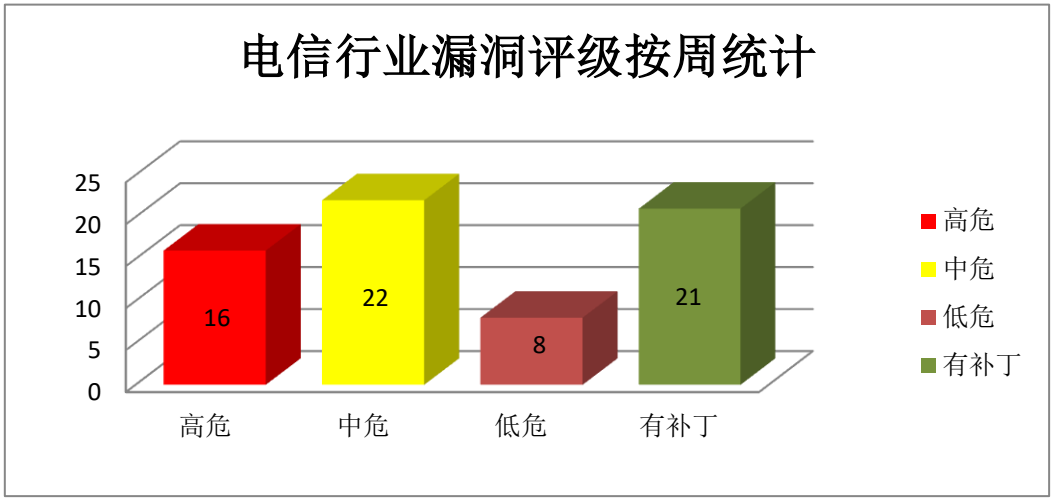

图 3 电信行业漏洞统计

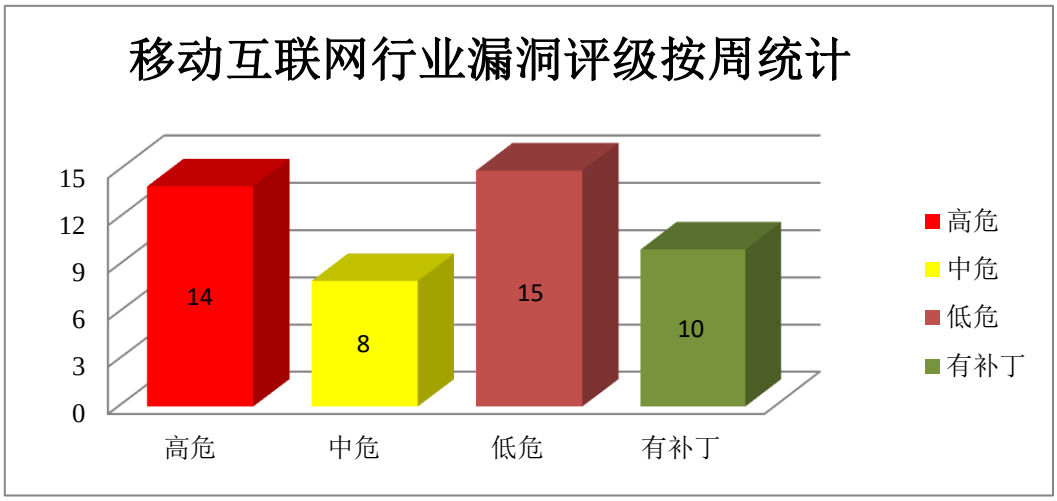

图 4 移动互联网行业漏洞统计

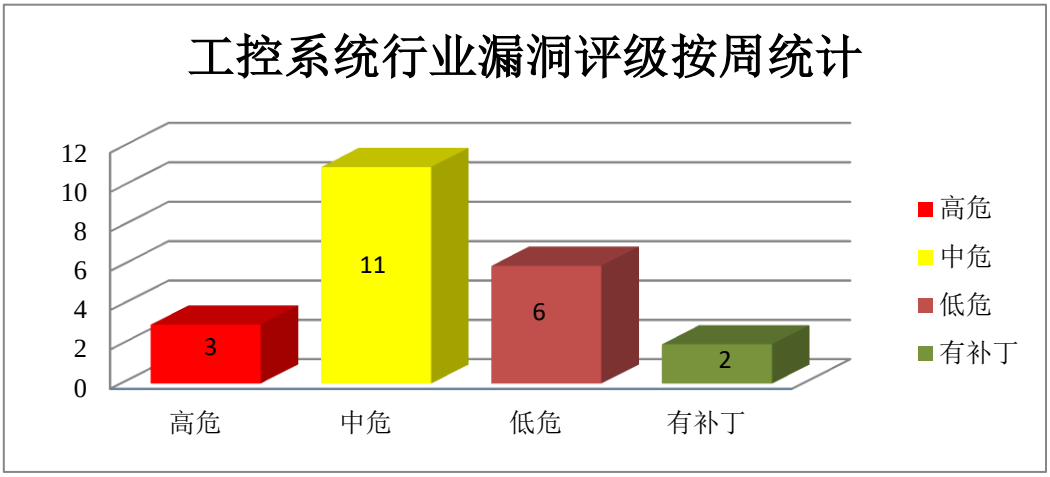

图 5 工控系统行业漏洞统计

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、 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，提升权限，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Google Android Media Framework 远程代码执行漏洞（CNVD-2021-19751）、Google Android 拒绝服务漏洞（CNVD-2021-19752）、Google Android Media Framework 权限提升漏洞（CNVD-2021-19750）、Google Android Framework 权限提升漏洞（CNVD-2021-19754、CNVD-2021-19753、CNVD-2021-19757、CNVD-2021-19756、CNVD-2021-19755）。其中，除 “Google Android 拒绝服务漏洞（CNVD-2021-19752）”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-2021-19751
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19750
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19754
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19753
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19752
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19757
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19756
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19755

2、Schneider Electric 产品安全漏洞

Schneider Electric Easergy T300 是法国施耐德电气（Schneider Electric）公司的一款用于电力行业的远程终端单元。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感信息，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Schneider Electric Easergy T300 访问控制不当漏洞（CNVD-2021-19765）、Schneider Electric Easergy T300 输入验证错误漏洞、Schneider Electric Easergy T300 跨站请求伪造漏洞、Schneider Electric Easergy T300 资源管理错误漏洞、Schneider Electric Easergy T300 加密问题漏洞、Schneider Electric Easergy T300 信息泄露漏洞（CNVD-2021-21474、CNVD-2021-21481、CNVD-2021-21478）。其中“Schneider Electric Easergy T300 访问控制不当漏洞（CNVD-2021-19765）”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-2021-19765
https://www.cnvd.org.cn/flaw/show/CNVD-2021-21472
https://www.cnvd.org.cn/flaw/show/CNVD-2021-21471
https://www.cnvd.org.cn/flaw/show/CNVD-2021-21475
https://www.cnvd.org.cn/flaw/show/CNVD-2021-21474
https://www.cnvd.org.cn/flaw/show/CNVD-2021-21479
https://www.cnvd.org.cn/flaw/show/CNVD-2021-21478
https://www.cnvd.org.cn/flaw/show/CNVD-2021-21481

3、Cisco 产品安全漏洞

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 Catalyst 9000 是一个交换机。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管理员权限，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco IOS XE OS 命令注入漏洞、Cisco IOS XE 拒绝服务漏洞（CNVD-2021-22166、CNVD-2021-22190）、Cisco IOS XE 缓冲区溢出漏洞、Cisco IOS XE 任意代码执行漏洞（CNVD-2021-22189）、Cisco IOS XE 权限提升漏洞（CNVD-2021-22457）、Cisco IOS XE IOx 命令注入漏洞、Cisco Catalyst 9000 拒绝服务漏洞。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-2021-22167
https://www.cnvd.org.cn/flaw/show/CNVD-2021-22166
https://www.cnvd.org.cn/flaw/show/CNVD-2021-22186
https://www.cnvd.org.cn/flaw/show/CNVD-2021-22189
https://www.cnvd.org.cn/flaw/show/CNVD-2021-22190
https://www.cnvd.org.cn/flaw/show/CNVD-2021-22454

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22459

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22457

4、Palo Alto Networks 产品安全漏洞

Palo Alto Networks GlobalProtect 是美国 Palo Alto Networks 公司的一套网络防护软件。该软件可提供防火墙监控及威胁预防等功能。Palo Alto Networks PAN-OS 是一套为其防火墙设备开发的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问受保护的资源、执行任意 OS 命令、导致缓冲区溢出等。

CNVD 收录的相关漏洞包括：Palo Alto Networks PAN-OS 数据伪造问题漏洞、Palo Alto Networks PAN-OS OS 命令注入漏洞（CNVD-2021-22171、CNVD-2021-22172）、Palo Alto Networks PAN-OS 缓冲区溢出漏洞（CNVD-2021-22178、CNVD-2021-22169）、Palo Alto Networks PAN-OS 操作系统命令注入漏洞（CNVD-2021-22180、CNVD-2021-22179）、Palo Alto Networks GlobalProtect 竞争条件问题漏洞。其中，除 “Palo Alto Networks GlobalProtect 竞争条件问题漏洞”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-2021-22173

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22172

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22171

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22169

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22181

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22180

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22179

https://www.cnvd.org.cn/flaw/show/CNVD-2021-22178

5、Bitweaver 跨站脚本漏洞（CNVD-2021-22579）

Bitweaver 是一款免费、开源 Web 应用程序框架和内容管理系统。本周，Bitweaver 被披露存在跨站脚本漏洞。远程攻击者可通过/users/admin/index.php URI 利用该漏洞注入 JavaScript。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-2021-22579

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-2021-19771	Open Solutions for Education openSIS SQL 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://github.com/OS4ED/openSIS-Responsive-Design/commit/28f9cbc943422d76ab2730f18ee279557be6b1c7
CNVD-2021-20210	Facebook Proxygen 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/facebook/proxygen/commit/f43b134cc5c19d8532e7fb670a1c02e85f7a8d4f
CNVD-2021-20272	多款 TP-Link 产品缓冲区溢出漏洞	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.tp-link.com/
CNVD-2021-20278	D-Link DIR-825 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.dlink.ru/ru/download2/5/19/2354/441/
CNVD-2021-20280	Huawei eCNS280 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://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210113-02-dos-en
CNVD-2021-20290	Adobe Magento 安全缓解绕过漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://helpx.adobe.com/security/products/magento/apsb20-22.html
CNVD-2021-21924	多款 MobileIron 产品远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.mobileiron.com/en/blog/mobileiron-security-updates-available
CNVD-2021-22127	WordPress wp-hotel-booking plugin 反序列化漏洞	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-hotel-booking/#developers
CNVD-2021-22136	F5 BIG-IP 越权访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K54431371
CNVD-2021-22157	SAP NetWeaver AS Java 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=547426775

小结：本周，Google 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，导致拒绝服务等。此外，Schneider Electric、Cisco、Palo Alto Networks 等多款产品被披露存在多个漏洞，攻击者可利用漏洞访问受保护的资源，访问

敏感信息，获取管理员权限，执行任意代码，导致拒绝服务和缓冲区溢出等。另外，Bitweaver 被披露存在跨站脚本漏洞。远程攻击者可通过/users/admin/index.php URI 利用该漏洞注入 JavaScript。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、Froala WYSIWYG HTML Editor 跨站脚本漏洞

验证描述

Froala WYSIWYG HTML Editor 是美国 Froala 公司的一款基于 Web 的 WYSIWYG 富文本编辑器。

Froala WYSIWYG HTML Editor 3.0.6 版本至 3.1.1 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://packetstormsecurity.com/files/158300/Froala-WYSIWYG-HTML-Editor-3.1.1-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-21927

信息提供者

恒安嘉新（北京）科技股份公司

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. 思科解决了 Windows、macOS Jabber 客户端中的严重错误

思科已解决了一个严重的任意程序执行漏洞，该漏洞影响了适用于 Windows，mac OS，Android 和 iOS 的多个版本的 Cisco Jabber 客户端软件。

参考链接：https://www.bleepingcomputer.com/news/security/cisco-addresses-critical-bug-in-windows-macos-jabber-clients/

2. Microsoft 修复了 Windows PSExec 提权漏洞

Microsoft 已修复 PsExec 实用程序中的一个漏洞，该漏洞允许本地用户在 Windows 设备上获得提升的特权。PsExec 是 Sysinternals 实用程序，旨在使管理员能够在远程计

算机上执行各种活动。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-fixes-windows-psexec-privilege-elevation-vulnerability/

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