国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 06 月 07 日-2021 年 06 月 13 日　　2021 年第 23 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 602 个，其中高危漏洞 227 个、中危漏洞 317 个、低危漏洞 58 个。漏洞平均分值为 6.21。本周收录的漏洞中，涉及 0day 漏洞 300 个（占 50%），其中互联网上出现“BloofoxCMS 跨站请求伪造漏洞 、emlog 路径遍历漏洞（CNVD-2021-39975）”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 3991 个，与上周（3759 个）环比增加 6%。

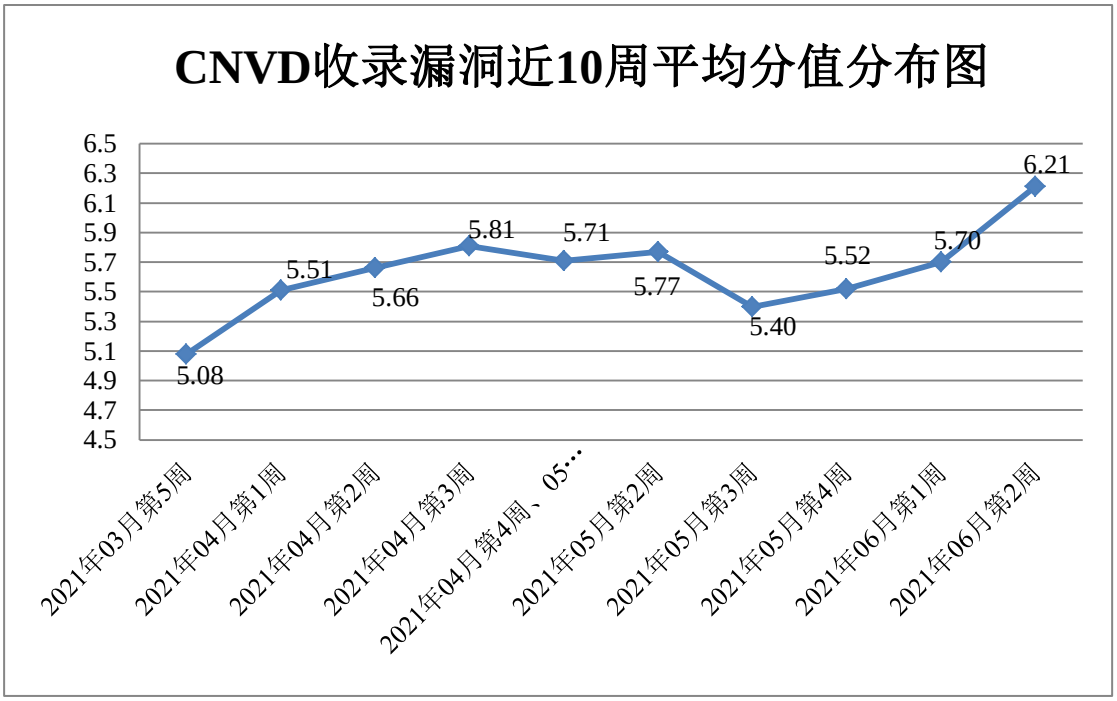

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 31 起，向基础电

信企业通报漏洞事件 17 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 211 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 40 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 31 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：

珠海金山办公软件有限公司、中兴保全股份有限公司、中科富创（北京）科技有限公司、中国电信集团公司、浙江大华技术股份有限公司、长沙市云研网络科技有限公司、长沙市同迅计算机科技有限公司、长沙米拓信息技术有限公司、运城市盘石网络科技有限公司、友讯电子设备（上海）有限公司、优刻得科技股份有限公司、新天科技股份有限公司、无锡城安信息科技有限公司、天津神州浩天科技有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、四川天健世纪科技有限公司、深圳市中科网威科技有限公司、深圳市网域科技技术有限公司、深圳市锐明技术股份有限公司、深圳市利谱信息技术有限公司、深圳市吉祥腾达科技有限公司、深圳市共济科技有限公司、深圳市奥联科技有限公司、深圳亮钻科技有限公司、深圳警翼智能科技股份有限公司、深圳华视美达信息技术有限公司、深圳奥联信息安全技术有限公司、深信服科技股份有限公司、上海纽盾科技股份有限公司、上海金慧软件有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海二三四五移动科技有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、陕西硅峰网络科技有限公司、任子行网络技术股份有限公司、欧姆龙自动化（中国）有限公司、南通润邦网络科技有限公司、南宁旭东网络科技有限公司、南宁小橙科技有限公司、理光（中国）投资有限公司、廊坊市极致网络科技有限公司、科大讯飞股份有限公司、金砖通讯科技股份有限公司、金蝶软件（中国）有限公司、江阴市领悟信息技术有限公司、江苏瑞丰信息技术股份有限公司、江苏怀业信息技术股份有限公司、江苏固德威电源科技股份有限公司、吉翁电子（深圳）有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、湖南畅乘科技有限公司、湖北点点点科技有限公司、洪湖尔创网联信息技术有限公司、河南礼恰网络科技有限公司、广州红帆科技有限公司、广东精工智能系统有限公司、高通公司、福建四创软件有限公司、东莞市通天星软件科技有限公司、戴尔（中国）有限公司、成都星锐蓝海网络科技有限公司、成都万江港利科技股份有限公司、成都强时科技有限公司、畅捷通信息技术股份有限公司、博威特网络技术（上海）有限公司、北京中控科技发展有限公司、北京中创视讯科技有限公司、北京智慧远景科技产业有限公司、北京原创先锋网络科技发展有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京信达网安科技有限公司、北京五一视界数字孪生科技股份有限公司、北京万户网络技术有限公司、北京盛世星火教育科技有限责任公司、北京圣博润高新技术股份有限公司、北京普华智深科技有限公司、北京猎鹰安全科技有限公司、北京科蓝软件

系统股份有限公司、北京金和网络股份有限公司、北京合力华彩科技有限公司、北京飞书科技有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、安美世纪（北京）科技有限公司、爱普生（中国）有限公司、上海程江科技中心、台达集团、商合行、柯尼卡美能达集团、狂雨小说 cms、zengcms、xhdcrm、ShirneCMS、SEMCMS、RPCMS、osgeo、KiteCMS、HadSky、Fulvio Ricciardi - Lecce、FasterXML、EacooPHP、CatfishCMS、BlueCMS、3Com 和 XHCMS。

本周，CNVD 发布了《Microsoft 发布 2021 年 6 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6516

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、华为技术有限公司、新华三技术有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。广州易东信息安全技术有限公司、南京众智维信息科技有限公司、北京信联科汇科技有限公司、贵州多彩宝互联网服务有限公司、北京山石网科信息技术有限公司、重庆贝特计算机系统工程有限公司、河南灵创电子科技有限公司、江西省掌控者信息安全技术有限公司、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、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、北京远禾科技有限公司、广州安亿信软件科技有限公司、长春嘉诚信息技术股份有限公司、星云博创科技有限公司、南京树安信息技术有限公司、浙江御安信息技术有限公司、上海市信息安全测评认证中心、武汉绿色网络信息服务有限责任公司、北京君云天下科技有限公司、江苏晟晖信息科技有限公司、山东云天安全技术有限公司、湖北珞格科技发展有限公司、中移（杭州）信息技术有限公司、重庆都会信息科技有限公司、日照天鉴网络科技有限公司、小安（北京）科技有限公司、中安网盾（广州）信息科技有限公司、广州铂豪万钧电子科技有限公司、广州百蕴启辰科技有限公司、江苏智慧安全可信技术研究院及其他个人白帽子向 CNVD 提交了 3991 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 2115 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）	1062	1062
奇安信网神（补天平台）	529	529
上海交大	524	524
阿里云计算有限公司	313	0

哈尔滨安天科技集团股份有限公司	267	0
华为技术有限公司	168	0
新华三技术有限公司	144	0
恒安嘉新（北京）科技股份公司	128	0
北京神州绿盟科技有限公司	126	6
北京天融信网络安全技术有限公司	102	3
深信服科技股份有限公司	93	3
北京启明星辰信息安全技术有限公司	38	38
卫士通信息产业股份有限公司	32	0
北京奇虎科技有限公司	32	32
北京数字观星科技有限公司	13	0
远江盛邦（北京）网络安全科技股份有限公司	10	10
北京长亭科技有限公司	6	6
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）	5	0
北京知道创宇信息技术股份有限公司	5	0
内蒙古奥创科技有限公司	2	2
广州易东信息安全技术有限公司	545	545
南京众智维信息科技有限公司	201	201
北京信联科汇科技有限公司	81	81
贵州多彩宝互联网服务有限公司	32	32
北京山石网科信息技术有限公司	21	21

重庆贝特计算机系统工程有限公司	19	19
河南灵创电子科技有限公司	19	19
江西省掌控者信息安全技术有限公司	18	18
河南信安世纪科技有限公司	17	17
杭州迪普科技股份有限公司	13	0
中国电信股份有限公司网络安全产品运营中心	13	0
北京天地和兴科技有限公司	12	12
西门子（中国）有限公司	9	0
山东泽鹿安全技术有限公司	9	9
武汉明嘉信信息安全检测评估有限公司	8	8
北京安帝科技有限公司	6	6
北京远禾科技有限公司	6	6
广州安亿信软件科技有限公司	4	4
长春嘉诚信息技术股份有限公司	4	4
星云博创科技有限公司	4	4
南京树安信息技术有限公司	3	3
浙江御安信息技术有限公司	3	3
上海市信息安全测评认证中心	3	3
武汉绿色网络信息服务有限责任公司	2	2
北京君云天下科技有限公司	2	2
江苏晟晖信息科技有限公司	2	2

山东云天安全技术有限公司	1	1
湖北珞格科技发展有限公司	1	1
中移（杭州）信息技术有限公司	1	1
重庆都会信息科技有限公司	1	1
日照天鉴网络科技有限公司	1	1
小安（北京）科技有限公司	1	1
中安网盾（广州）信息科技有限公司	1	1
广州铂豪万钧电子科技有限公司	1	1
广州百蕴启辰科技有限公司	1	1
江苏智慧安全可信技术研究院	1	1
CNCERT 贵州分中心	1	1
个人	744	744
报送总计	5410	3991

本周漏洞按类型和厂商统计

本周，CNVD 收录了 602 个漏洞。应用程序 220 个，WEB 应用 201 个，网络设备（交换机、路由器等网络端设备）135 个，安全产品 16 个，智能设备（物联网终端设备）16 个，操作系统 14 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	220
WEB 应用	201
网络设备（交换机、路由器等网络端设备）	135
安全产品	16
智能设备（物联网终端设备）	16
操作系统	14

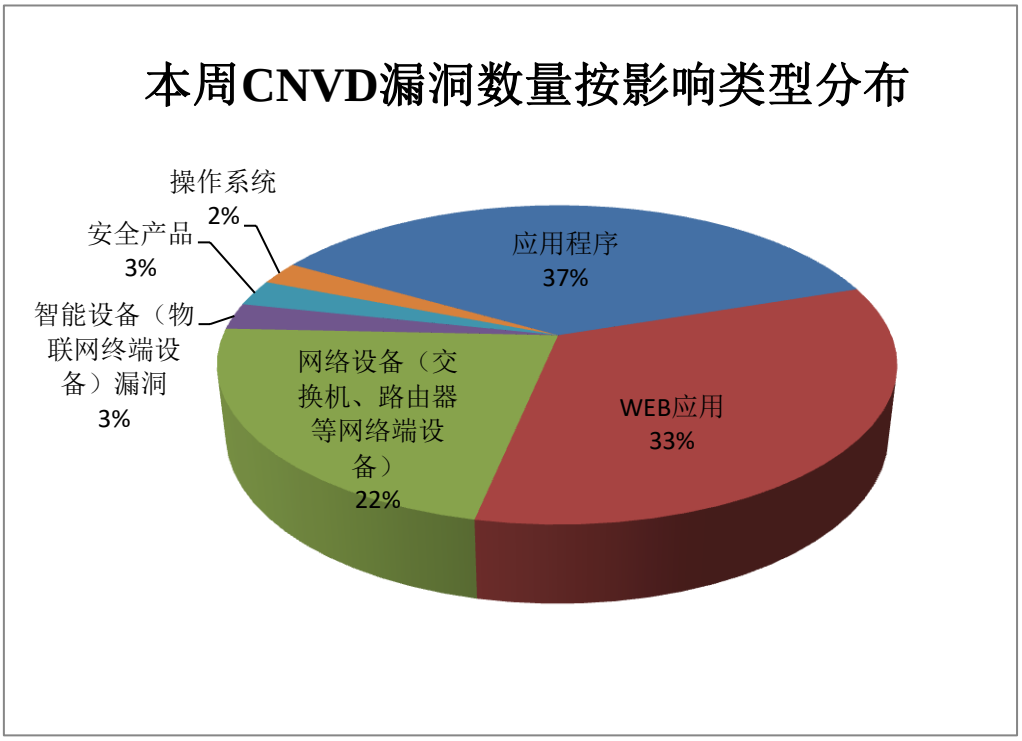

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Google、北京星网锐捷网络技术有限公司等多家厂商的产品，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	Cisco	81	14%
2	Google	31	5%
3	北京星网锐捷网络技术有限公司	17	3%
4	Oracle	16	3%
5	Adobe	15	2%
6	IBM	15	2%
7	深圳市吉祥腾达科技有限公司	13	2%
8	FFmpeg	11	2%
9	Microsoft	10	2%
10	其他	393	65%

本周行业漏洞收录情况

本周，CNVD 收录了 117 个电信行业漏洞，15 个移动互联网行业漏洞，14 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2021-41111）、Siemens SIMATIC RFID Readers 拒绝服务漏洞、Cisco RV110W/RV130/RV130W/RV215W 命令注入漏洞”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/

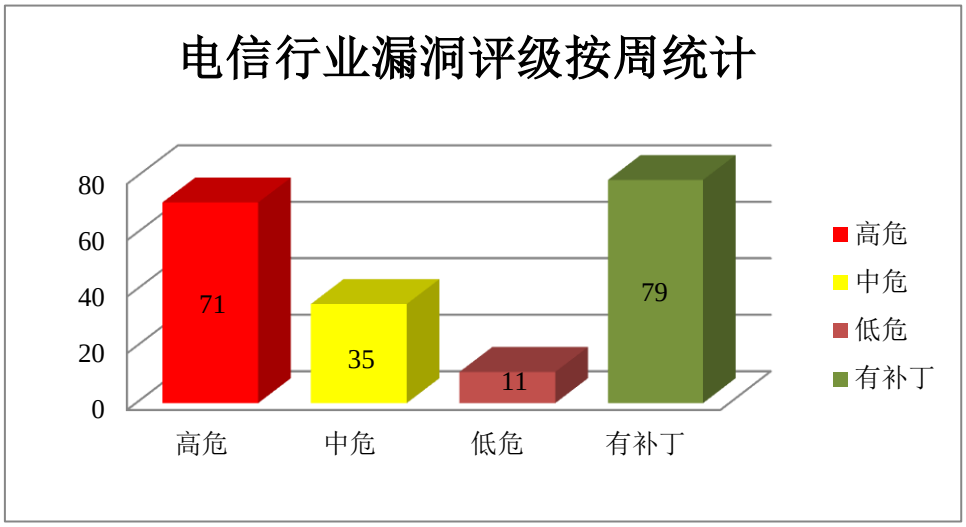

图 3 电信行业漏洞统计

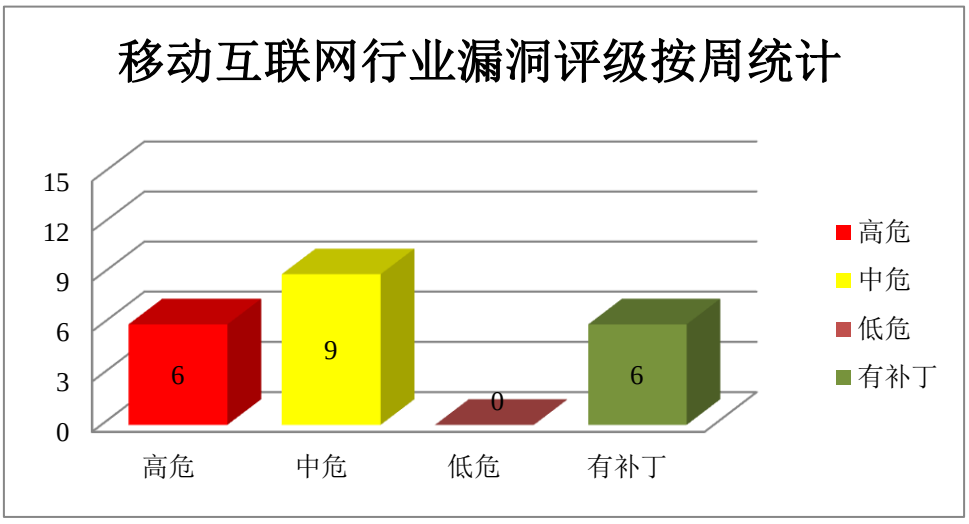

图 4 移动互联网行业漏洞统计

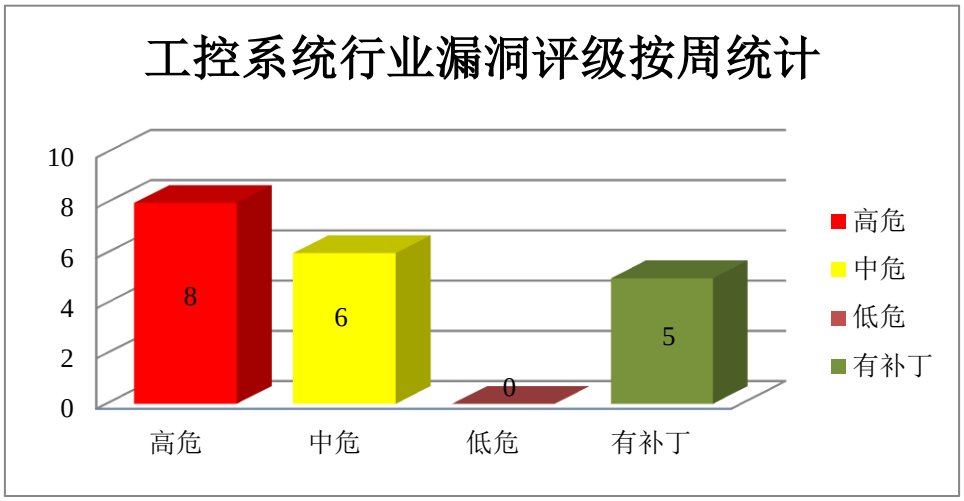

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。Adobe After Effects（简称“AE”）是 Adobe 公司推出的一款图形视频处理软件，适用于从事设计和视频特技的机构，包括电视台、动画制作公司、个人后期制作工作室以及多媒体工作室。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代码。

CNVD 收录的相关漏洞包括：Adobe Photoshop 缓冲区溢出漏洞（CNVD-2021-41059）、Adobe After Effects 缓冲区溢出漏洞（CNVD-2021-41071、CNVD-2021-41070、CNVD-2021-41072）、Adobe After Effects 堆缓冲区溢出漏洞（CNVD-2021-41067、CNVD-2021-41066、CNVD-2021-41069、CNVD-2021-41068）。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-2021-41059

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41067

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41066

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41071

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41070

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41069

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41068

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41072

2、Siemens 产品安全漏洞

Siemens Solid Edge 是德国 Siemens 公司的一款三维 CAD 软件。Mendix SAML

Module 允许使用 SAML 对云应用程序中的用户进行身份验证。该模块可以与任何支持 SAML2.0 或 Shibboleth 的身份提供者进行通信。Siemens Jt2go 是德国 Siemens 公司的一款 JT 文件查看器。Siemens Teamcenter Visualization 是一个可为设计 2D、3D 场景提供团队协作功能的软件。SIMATIC RF185C、RF186C/CI 和 RF188C/CI 是用于将图像识别系统直接连接到 PROFINET IO/以太网和 OPC UA 的通信模块。SIMATIC RF300R 是一款紧凑型 RFID 读卡器。Simcenter Femap 是一种高级仿真应用程序，用于创建、编辑和检查复杂产品或系统的有限元模型。Siemens SmartVNC 是德国西门子（Siemens）公司的一个工控设备。提供一个访问 HMI 中的 smartserver 功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在当前进程的上下文中执行代码，造成拒绝服务情况。

CNVD 收录的相关漏洞包括：Siemens Solid Edge 越界写入漏洞（CNVD-2021-40500）、Siemens Mendix SAML Module 权限提升漏洞、Siemens JT2Go 和 Teamcenter Visualization 越界写入漏洞（CNVD-2021-40498）、Siemens SIMATIC RFID Readers 拒绝服务漏洞、Siemens Simcenter Femap 越界写入漏洞（CNVD-2021-40502）、Siemens Solid Edge 越界写入漏洞（CNVD-2021-40501）、Siemens Simcenter Femap 越界写入漏洞、Siemens SmartVNC 越界内存访问漏洞。其中，除“Siemens SmartVNC 越界内存访问漏洞”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-2021-40500

https://www.cnvd.org.cn/flaw/show/CNVD-2021-40499

https://www.cnvd.org.cn/flaw/show/CNVD-2021-40498

https://www.cnvd.org.cn/flaw/show/CNVD-2021-40497

https://www.cnvd.org.cn/flaw/show/CNVD-2021-40502

https://www.cnvd.org.cn/flaw/show/CNVD-2021-40501

https://www.cnvd.org.cn/flaw/show/CNVD-2021-40503

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41246

3、Google 产品安全漏洞

Google Android 是一款以 Linux 为基础的开源操作系统。Chrome 是由 Google 开发的一款 Web 浏览工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面利用堆损坏，进行特权升级。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2021-41110、CNVD-2021-41113、CNVD-2021-41112、CNVD-2021-41111、CNVD-2021-41115）、Google Android 输入验证错误漏洞（CNVD-2021-41116）、Google Chrome 释放后重用漏洞（CNVD-2021-41140、CNVD-2021-41139）。其中，“Google Android 权限提升漏洞（CNVD-2021-41110、CNVD-2021-41111）、Google Android 输入验证错误漏洞（CNVD-20

21-41116）”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-2021-41110

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41113

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41112

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41111

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41116

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41115

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41140

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41139

4、Microsoft 产品安全漏洞

Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。Paint 3D 是 Windows 10 免费附带的创意应用程序，支持用户使用 2D 和 3D 工具创建创意项目。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在目标主机上执行代码，欺骗内容并诱导用户相信该网站的合法性，同时结合网页服务中的其他漏洞发起攻击。

CNVD 收录的相关漏洞包括：Microsoft SharePoint Server 远程代码执行漏洞（CNVD-2021-41120、CNVD-C-2021-142456、CNVD-2021-41118）、Microsoft SharePoint Server 欺骗漏洞（CNVD-2021-41122）、Microsoft SharePoint Server 信息泄露漏洞（CNVD-2021-41121）、Microsoft Paint 3D 远程代码执行漏洞（CNVD-2021-41127、CNVD-2021-41126、CNVD-2021-41125）。其中，“Google Android 权限提升漏洞（CNVD-2021-41110、CNVD-2021-41111）、Google Android 输入验证错误漏洞（CNVD-2021-41116）”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-2021-41120

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41119

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41118

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41122

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41121

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41127

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41126

https://www.cnvd.org.cn/flaw/show/CNVD-2021-41125

5、D-Link DIR-868L 信息泄露漏洞

D-Link DIR-868L 是一款无线 AC1750 双频千兆云路由器。本周，D-Link DIR-868

L 被披露存在信息泄露漏洞。攻击者可通过反编译固件利用该漏洞访问固件并提取敏感数据。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-2021-41077

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-2021-40323	Dell EMC PowerScale OneFS 权限提升漏洞（CNVD-2021-40323）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/000185978
CNVD-2021-40324	D-Link DAP-2020 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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201
CNVD-2021-40512	labapart GattLib 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://github.com/labapart/gattlib/issues/219
CNVD-2021-40755	WellCMS 文件上传漏洞	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：http://www.wellcms.cn/read-27.html&&
CNVD-2021-40757	Advantech iView SQL 注入漏洞（CNVD-2021-40757）	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.advantech.tw/support/details/firmware?id=1-HIPU-183
CNVD-2021-40761	Accusoft ImageGear 缓冲区溢出漏洞（CNVD-2021-40761）	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.accusoft.com/products/imagegear-collection/
CNVD-2021-40767	Vembu BDR Suite 命令注入漏洞（CNVD-2021-40767）	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.vembu.com/vembu-bdr-suite/
CNVD-2021-40868	IBM QRadar SIEM 任意命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新:https://www.ibm.com/support/pages/node/6449668
CNVD-2021-	Mozilla Firefox 信息泄露漏	高	厂商已发布了漏洞修复程序，请及时

41087	洞（CNVD-2021-41087）		关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2021-23/
CNVD-2021-41086	F5 BIG-IQ 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://support.f5.com/csp/article/K06024431。

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Siemens、Google、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面利用堆损坏，进行特权升级，在当前进程的上下文中执行代码，造成拒绝服务情况等。另外，D-Link DIR-868L 被披露存在信息泄露漏洞。攻击者可通过反编译固件利用该漏洞访问固件并提取敏感数据。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、BloofoxCMS 跨站请求伪造漏洞

验证描述

BloofoxCMS 是一款基于 PHP + MySQL 的免费开源 Web 内容管理系统。

BloofoxCMS 0.5.2.1 版存在跨站请求伪造漏洞。攻击者可通过 mode=settings&page=editor 利用该漏洞更改任意文件内容。

验证信息

POC 链接：https://muteb.io/2020/12/29/BloofoxCMS-Multiple-Vulnerabilities.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-41074

信息提供者

华为技术有限公司

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. 微软 Office 组件中的 4 个漏洞允许攻击者将文档武器化

Check Point 的专家在 Microsoft Office 组件中发现了四个安全漏洞，攻击者可以利用这些漏洞来制作武器化的 Word 和 Excel 文档。

参考链接：https://securityaffairs.co/wordpress/118741/breaking-news/microsoft-office-

component-flaws.html

2. 半年内发现三星手机 17 个漏洞，可被用于间谍监听

一位白帽黑客向三星提交了多达 17 个漏洞，这些漏洞可能被用于间谍活动或提权控制系统。目前，三星正在修复这些漏洞。

参考链接：https://www.freebuf.com/news/277225.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