国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 02 月 22 日-2021 年 02 月 28 日　　2021 年第 8 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 502 个，其中高危漏洞 205 个、中危漏洞 241 个、低危漏洞 56 个。漏洞平均分值为 5.98。本周收录的漏洞中，涉及 0day 漏洞 296 个（占 59%），其中互联网上出现“WordPress Plugin Autoptimize Authenticated 任意文件上传漏洞、Apache MyFaces 跨站请求伪造漏洞”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 4894 个，与上周（4438 个）环比增加 10%。

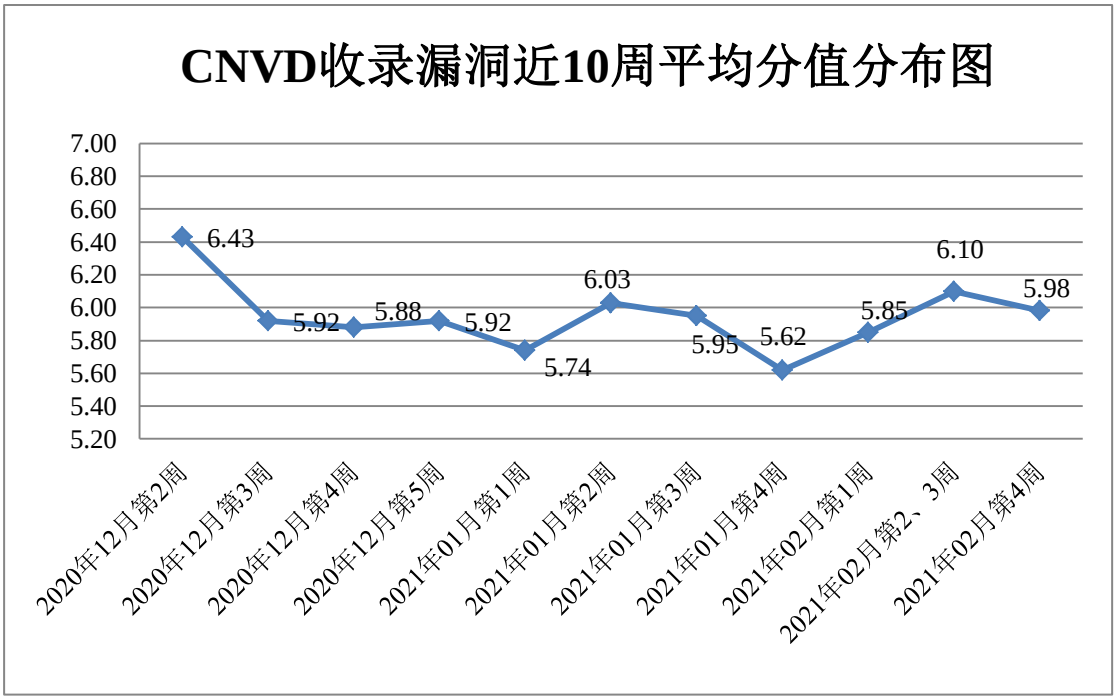

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 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 463 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 62 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 20 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：

松下电器（中国）有限公司、太原迅易科技有限公司、三星（中国）投资有限公司、浙江浙大中控信息技术有限公司、福建易视科技有限公司、深圳（北京）感闻科技有限公司、中国联盟网集团股份有限公司、深圳市任想科技有限公司、深圳零壹信息科技有限责任公司、四川迅睿云软件开发有限公司、茉柏枘（上海）软件科技有限公司、中国中信集团有限公司、上海嵩恒网络科技股份有限公司、北京海腾时代科技有限公司、珠海金山办公软件有限公司、绎览信息技术（上海）有限公司、杭州奇亿云计算有限公司、馥鸿科技股份有限公司、温州优谷科技有限公司、方正集团、深圳致安视科技有限公司、锐捷网络股份有限公司、漳州市芗城帝兴软件开发有限公司、安美世纪（北京）科技有限公司、海南赞赞网络科技有限公司、蚌埠依爱消防电子有限责任公司、宁波高新区奥凯网络科技有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、杭州海康威视数字技术股份有限公司、山东威尔数据股份有限公司、上海装盟信息科技有限公司、南京纳龙科技有限公司、绎览信息技术（上海）有限公司、深圳市驱动人生科技股份有限公司、迈普通信技术股份有限公司、邦奇智能科技（上海）股份有限公司、罗克韦尔自动化（中国）有限公司、東科技有限公司、深圳市吉祥腾达科技有限公司、优酷信息技术（北京）有限公司、上海二三四五网络科技有限公司、友讯电子设备（上海）有限公司、厦门科拓通讯技术股份有限公司、上海浪擎信息科技有限公司、深圳市明源云科技有限公司、深圳市宏电技术股份有限公司、上海畅指网络科技有限公司、北京亿赛通科技发展有限责任公司、上海艺觉网络科技有限公司、兴化市信网信息咨询服务部、北京金和网络股份有限公司、深圳市迅雷网络技术有限公司、台达电子企业管理(上海)有限公司、厦门科汛软件有限公司、微宏软件技术（杭州）有限公司、常州企轩信息技术有限公司、国晋信息科技有限公司、北京星网锐捷网络技术有限公司、上海牛迈网络科技有限公司、上海上业信息科技有限公司、宁波易龙计算机科技有限公司、广州齐博网络科技有限公司、上海牛之云网络科技有限公司、北京搜狐互联网信息服务有限公司、北京酷我科技有限公司、北京百度网讯科技有限公司、江苏固德威电源科技股份有限公司、鹏为软件股份有限公司、北京网御星云信息技术有限公司、科大讯飞股份有限公司、广州瀚德网络科技有限公司、北京映翰通网络技术股份有限公司、用友网络科技股份有限公司、深圳市天视通电子科技有限公司、苏州三三云网络科技有限公司、内蒙古开企科技有限公司、广州市璐华计算机科技有限公司、北京我知科技有限公司、南京三商电脑软件开发有限公司、厦门一指通智能科技有限公司、睿谷信息、成都零起飞网络、海洋 CMS、百家 CMS、里程密 PHP 开源博客系统、iCMS、Jpom、DCS Synthesis、draytekfae、

FANUC、Mblog、XYCMS、Apache Friends 和 ZZCMS。

本周，CNVD 发布了《关于 VMware 多款产品存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6086

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天科技集团股份有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、北京山石网科信息技术有限公司、安徽长泰信息安全服务有限公司、山东新潮信息技术有限公司、南京众智维信息科技有限公司、上海犀点意象网络科技有限公司、北京天地和兴科技有限公司、河南信安世纪科技有限公司、西安交大捷普网络科技有限公司、泽鹿安全、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、远江盛邦（北京）网络安全科技股份有限公司、山东华鲁科技发展股份有限公司、北京华云安信息技术有限公司、北京顶象技术有限公司、江苏保旺达软件技术有限公司、京东云安全、贵州多彩宝互联网服务有限公司、上海观安信息技术股份有限公司、杭州海康威视数字技术股份有限公司、杭州天谷信息科技有限公司、神州网安（北京）信息科技有限公司、北京君云天下科技有限公司、北京惠而特科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、郑州云智信安安全技术有限公司、北京信联科汇科技有限公司、中国工商银行软件开发中心、上海匡创信息技术有限公司、北京长亭科技有限公司、广州市蓝爵计算机科技有限公司、工业信息安全(四川)创新中心有限公司、北京小米科技有限责任公司、杭州安信检测技术有限公司、国网山东省电力公司、广东东福信息技术有限公司、北京瑾逸海阔科技有限公司、武汉明嘉信信息安全检测评估有限公司、北京智游网安科技有限公司、广州安亿信软件科技有限公司及其他个人白帽子向 CNVD 提交了 4894 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 3075 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）	1929	1929
上海交大	677	677
奇安信网神（补天平台）	469	469
北京天融信网络安全技术有限公司	391	4
哈尔滨安天科技集团股份有限公司	244	0
北京神州绿盟科技有限公司	212	28

深信服科技股份有限公司	99	0
华为技术有限公司	89	0
北京数字观星科技有限公司	77	0
新华三技术有限公司	77	0
中国电信集团系统集成有限责任公司	61	61
北京奇虎科技有限公司	41	25
西安四叶草信息技术有限公司	28	28
中国电信股份有限公司网络安全产品运营中心	20	0
北京知道创宇信息技术股份有限公司	7	0
恒安嘉新(北京)科技股份公司	3	0
北京启明星辰信息安全技术有限公司	2	2
山东云天安全技术有限公司	232	232
北京山石网科信息技术有限公司	110	110
北京华顺信安科技有限公司	105	0
安徽长泰信息安全服务有限公司	99	99
山东新潮信息技术有限公司	85	85
南京众智维信息科技有限公司	83	83
上海犀点意象网络科技有限公司	79	79
北京天地和兴科技有限公司	49	49
河南信安世纪科技有限公司	32	32
西安交大捷普网络科技有限公司	30	30
泽鹿安全	30	30
河南灵创电子科技有限公司	26	26
山石网科通信技术股份有限公司	24	24
远江盛邦（北京）网络安全科技股份有限公司	15	15
山东华鲁科技发展股份有限公司	14	14
北京华云安信息技术有限公司	13	13
北京顶象技术有限公司	12	12

江苏保旺达软件技术有限公司	11	11
京东云安全	11	11
贵州多彩宝互联网服务有限公司	9	9
上海观安信息技术股份有限公司	6	6
杭州海康威视数字技术股份有限公司	5	5
杭州天谷信息科技有限公司	5	5
神州网安（北京）信息科技有限公司	3	3
北京君云天下科技有限公司	3	3
北京惠而特科技有限公司	3	3
北京云科安信科技有限公司（Seraph 安全实验室）	3	3
郑州云智信安安全技术有限公司	2	2
北京信联科汇科技有限公司	2	2
中国工商银行软件开发中心	2	2
上海匡创信息技术有限公司	2	2
北京长亭科技有限公司	2	2
广州市蓝爵计算机科技有限公司	1	1
工业信息安全(四川)创新中心有限公司	1	1
北京小米科技有限责任公司	1	1
杭州安信检测技术有限公司	1	1
国网山东省电力公司	1	1
广东东福信息技术有限公司	1	1
北京瑾逸海阔科技有限公司	1	1
武汉明嘉信信息安全检测评估有限公司	1	1
北京智游网安科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
CNCERT 重庆分中心	18	18
CNCERT 上海分中心	16	16
CNCERT 海南分中心	15	15
CNCERT 天津分中心	15	15
CNCERT 宁夏分中心	12	12
CNCERT 青海分中心	11	11
CNCERT 山西分中心	10	10

CNCERT 山东分中心	8	8
CNCERT 湖南分中心	7	7
CNCERT 浙江分中心	4	4
CNCERT 四川分中心	2	2
CNCERT 甘肃分中心	1	1
CNCERT 河南分中心	1	1
个人	539	539
报送总计	6202	4894

本周漏洞按类型和厂商统计

本周，CNVD 收录了 502 个漏洞。应用程序 231 个，WEB 应用 168 个，网络设备（交换机、路由器等网络端设备）61 个，操作系统 20 个，安全产品 18 个，智能设备（物联网终端设备）3 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	231
WEB 应用	168
网络设备（交换机、路由器等网络端设备）	61
操作系统	20
安全产品	18
智能设备（物联网终端设备）	3
数据库	1

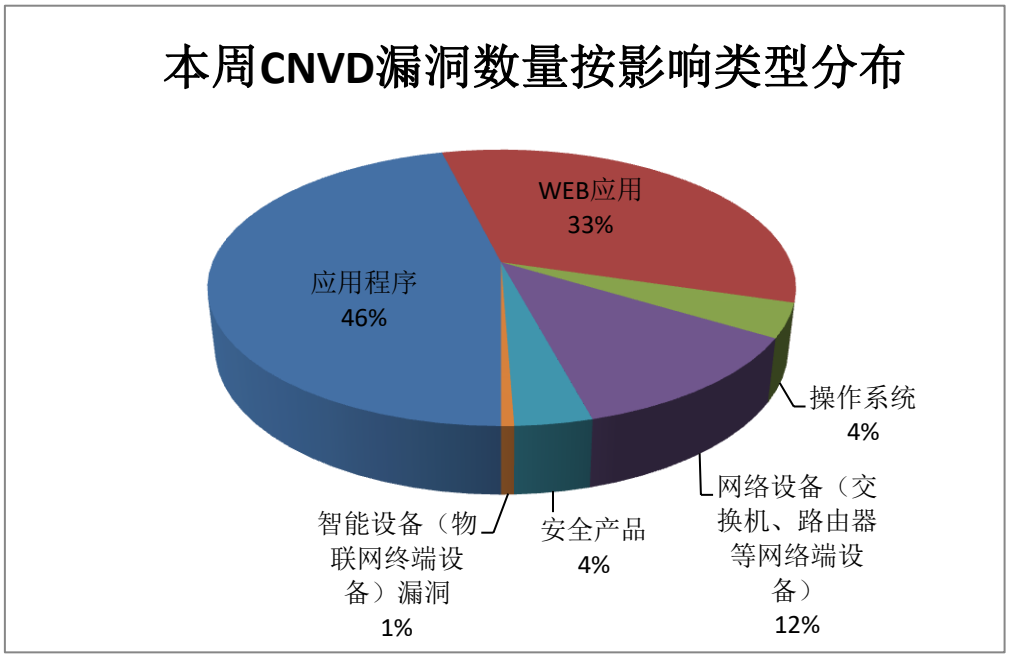

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Fiberhome、IBM、Adobe 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	Fiberhome	27	6%
2	IBM	22	4%
3	Adobe	20	4%
4	SIEMENS	18	4%
5	Apache	17	3%
6	广东凯格科技有限公司	16	3%
7	Google	14	3%
8	Wireshark	11	2%
9	Cisco	11	2%
10	其他	346	69%

本周行业漏洞收录情况

本周，CNVD 收录了 55 个电信行业漏洞，34 个移动互联网行业漏洞，29 个工控行业漏洞（如下图所示）。其中，“Siemens DIGSI 4 权限提升漏洞、Cisco NX-OS 跨站请求伪造漏洞、Google Android Kernel 组件权限提升漏洞（CNVD-2021-12818）、Advantech iView SQL 注入漏洞（CNVD-2021-13242）、Cisco NX-OS 拒绝服务漏洞（CNVD-2021-13218）”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/

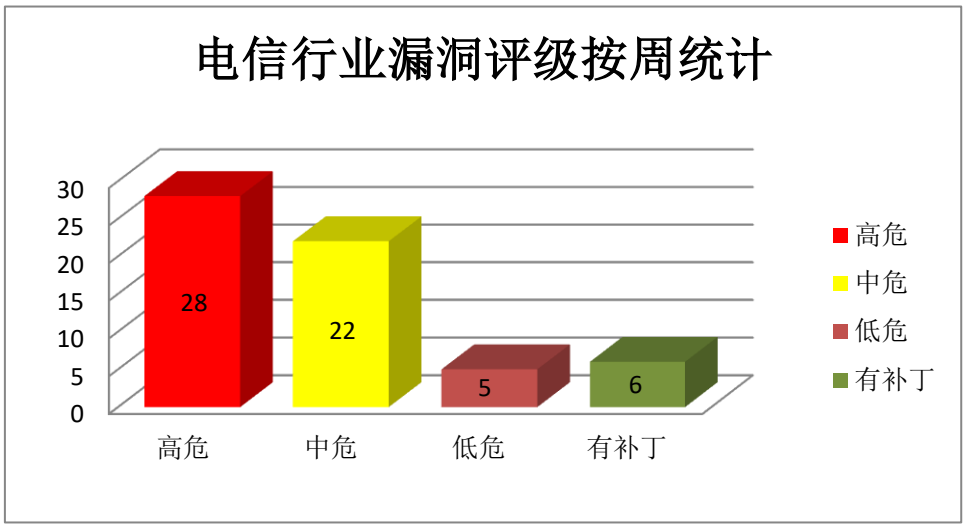

图 3 电信行业漏洞统计

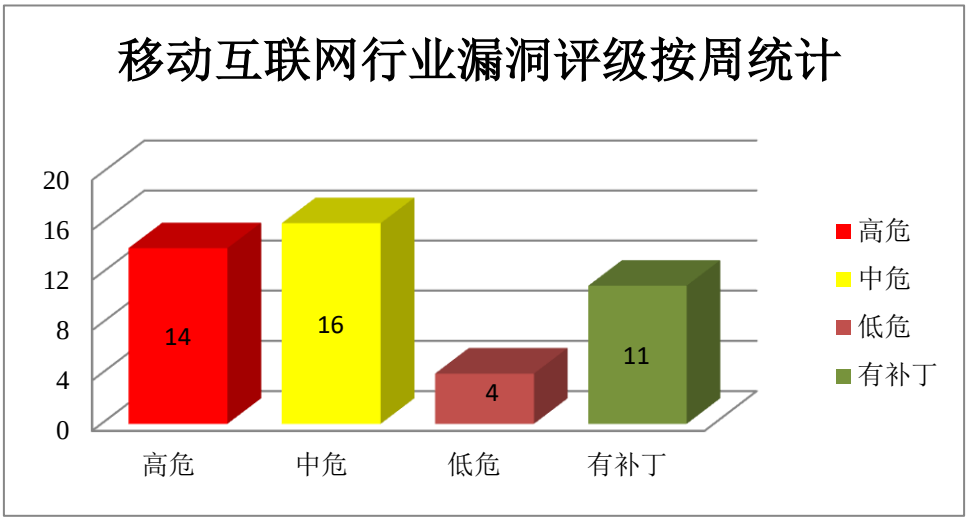

图 4 移动互联网行业漏洞统计

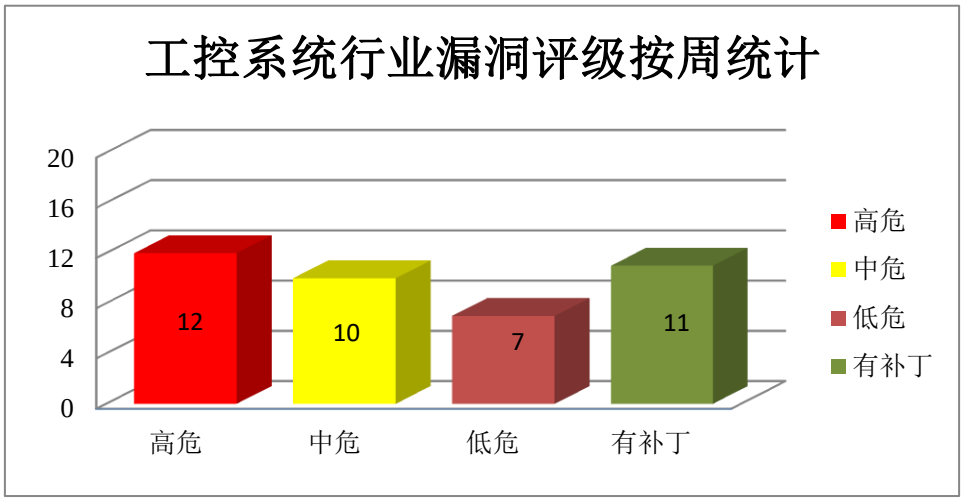

图 5 工控系统行业漏洞统计

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 Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：多款 Adobe 产品缓冲区溢出漏洞（CNVD-2021-11286、CNVD-2021-11285、CNVD-2021-11284、CNVD-2021-11287、CNVD-2021-11297）、多款 Adobe 产品越界写入漏洞（CNVD-2021-11289、CNVD-2021-11288）、多款 Adobe 产品越界读取漏洞（CNVD-2021-11292）。其中，除“多款 Adobe 产品越界写入漏洞（CNVD-2021-11288）、多款 Adobe 产品越界读取漏洞（CNVD-2021-11292）、多款 Adobe

产品缓冲区溢出漏洞（CNVD-2021-11297）”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-2021-11286
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11285
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11284
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11289
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11288
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11287
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11292
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11297

2、IBM 产品安全漏洞

IBM Security Verify Information Queue 是一个跨产品集成器，其利用 Kafka 技术和发布/订阅模型在 IBM 安全产品之间集成数据。IBM Planning Analytics 是美国 IBM 公司的一套业务规划分析解决方案。IBM Planning Analytics 是美国 IBM 公司的一套业务规划分析解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行未经授权的活动，获取敏感信息，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Security Verify Information Queue 信息泄露漏洞（CNVD-2021-11355、CNVD-2021-11360、CNVD-2021-11362）、IBM Security Verify Information Queue 权限提升漏洞、IBM Security Verify Information Queue 拒绝服务漏洞、IBM Security Verify Information Queue 会话固定漏洞、IBM Planning Analytics Workspace 信息泄露漏洞、IBM API Connect 跨站脚本执行漏洞。其中，“IBM API Connect 跨站脚本执行漏洞”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-2021-11355
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11360
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11358
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11357
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11364
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11362
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12642
https://www.cnvd.org.cn/flaw/show/CNVD-2021-13223

3、Siemens 产品安全漏洞

Siemens Jt2go 是一款 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。TIA Administrator 是一个基于 web 的框

架，它可以包含用于管理任务的不同功能模块，以及用于管理 SIMATIC 软件和许可证的功能。DIGSI 4 是 SIPROTEC 4 和 SIPROTEC 紧凑型保护装置的操作和配置软件。Siemens SINE CNMS 是新一代面向数字图书馆的网络管理系统企业号。Siemens SIMARIS configuration 在构建配电系统时支持全数字工程过程，从规划到成本计算和投标准备，再到符合标准的配电系统文件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获得持久性或潜在的升级权限，在受影响的系统上创建或覆盖任意文件，以系统权限执行代码等。

CNVD 收录的相关漏洞包括：Siemens JT2Go 和 Teamcenter Visualization 越界写入漏洞、Siemens JT2Go 和 Teamcenter Visualization 内存破坏漏洞（CNVD-2021-11823、CNVD-2021-11829）、Siemens JT2Go 和 Teamcenter Visualization 堆栈缓冲区溢出漏洞、Siemens TIA Administrator 权限提升漏洞、Siemens DIGSI 4 权限提升漏洞、Siemens SINEMA Server 和 SINE CNMS 目录遍历漏洞、Siemens SIMARIS configuration 不安全文件夹权限漏洞。其中，“Siemens TIA Administrator 权限提升漏洞、Siemens DIGSI 4 权限提升漏洞”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-2021-11824

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11823

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11829

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11828

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11833

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11832

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11835

https://www.cnvd.org.cn/flaw/show/CNVD-2021-12078

4、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Asylo 是一款用于开发 enclave 应用程序的开放且灵活的框架。Google Android 是美国谷歌（Google）和开放手持设备联盟（简称 oha）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，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Asylo 缓冲区溢出漏洞、Google Android Pixel 信息泄露漏洞（CNVD-2021-12814）、Google Chrome on iOS 注入漏洞、Google Android Kernel 组件权限提升漏洞（CNVD-2021-12818、CNVD-2021-12817、CNVD-2021-12816）、Google Android System 信息泄露漏洞（CNVD-2021-12820、CNVD-2021-12819）。其中“Google Android Kernel 组件权限提升漏洞（CNVD-2021-12818、CNVD-2021-12817、CNVD-2021-12816）”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-2021-12815
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12814
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12813
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12818
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12817
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12816
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12820
https://www.cnvd.org.cn/flaw/show/CNVD-2021-12819

5、Advantech WebAccess/SCADA 本地权限提升漏洞

Advantech WebAccess/SCADA 是 Advantech 公司的一套基于浏览器架构的 SCADA 软件。本周，Advantech WebAccess/SCADA 被披露存在本地权限提升漏洞。攻击者可利用该漏洞替换二进制文件或加载的模块，从而能以 NT SYSTEM 权限执行代码。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-2021-11308

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-2021-11313	NetMotion Mobility 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://www.netmotionsoftware.com/security/advisories/security-vulnerability-in-mobility-web-server-november-19-2020
CNVD-2021-12092	SolarWinds Orion Platform 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://documentation.solarwinds.com/en/Success_Center/orionplatform/content/release_notes/orion_platform_2020-2-4_release_notes.htm
CNVD-2021-12321	VMware ESXi OpenSLP 堆溢出漏洞	高	目前，VMware 官方已发布补丁修复此漏洞，CNVD 建议用户立即升级至最新版本：https://www.vmware.com/security/advisories/VMSA-2021-0002.html
CNVD-2021-12635	McAfee Web Gateway (MWG)权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kc.mcafee.com/corporate/index?

			page=content&id=SB10349
CNVD-2021-12656	Dell PowerScale OneFS 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://www.dell.com/support/kbdoc/en-us/000182873/dsa-2021-009-dell-powerscale-onefs-security-update-for-multiple-vulnerabilities
CNVD-2021-13201	SAP Commerce Cloud 远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=568460543
CNVD-2021-13212	F5 BIG-IP APM 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.f5.com/csp/article/K88162221
CNVD-2021-13217	Cisco NX-OS 跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nxapi-csrf-wRMzWL9z
CNVD-2021-13242	Advantech iView SQL 注入漏洞（CNVD-2021-13242）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.advantech.com/support/details/firmware?id=1-HIPU-183
CNVD-2021-12322	VMware vCenter Server 远程代码执行漏洞	高	目前，VMware 官方已发布补丁修复此漏洞，CNVD 建议用户立即升级至最新版本：https://www.vmware.com/security/advisories/VMSA-2021-00

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致拒绝服务。此外，IBM、Siemens、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获得持久性或潜在的升级权限，执行未经授权的活动，获取敏感信息，在受影响的系统上创建或覆盖任意文件，以系统权限执行代码，导致拒绝服务等。另外，Advantech WebAccess/SCADA 被披露存在本地权限提升漏洞。攻击者可利用该漏洞替换二进制文件或加载的模块，从而能以 NT SYSTEM 权限执行代码。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、Apache MyFaces 跨站请求伪造漏洞

验证描述

Apache MyFaces Trinidad 是美国阿帕奇（Apache）基金会的一款包含大量的企业级组件库并支持附件的 JSF 框架。

Apache MyFaces 中存在跨站请求伪造漏洞。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/161484/Apache-MyFaces-2.x-Cross-Site-Request-Forgery.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-13225

信息提供者

北京启明星辰信息安全技术有限公司

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. 英特尔发布 PROSet/无线软件 22.30.0 驱动更新，修复 Windows 蓝屏错误

英特尔发布了 Windows 10 的 PROSet/无线软件 22.30.0 新驱动，这次为微软最新操作系统的用户带来了一系列关键性的修复措施，并带来了四项改进，其中一项涉及到启动进入 Windows 后随机发生的 BSOD 蓝屏死机。

参考链接：https://www.cnbeta.com/articles/soft/1095381.htm

2. Mozilla 修补了 Firefox 中的错误 阻止跨站点 Cookie 跟踪

Mozilla 已经发布了最新版本的 Firefox 浏览器，该浏览器具有新的隐私保护功能，可以挤压跨站点 Cookie 跟踪，并且还提供了大量安全漏洞修复程序。

参考链接：https://threatpost.com/mozilla-firefox-bugs-cookie-tracking/164246/

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