国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 04 月 11 日-2022 年 04 月 17 日 **2022 年第 15 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 311 个，其中高危漏洞 108 个、中危漏洞 177 个、低危漏洞 26 个。漏洞平均分值为 6.00。本周收录的漏洞中，涉及 0day 漏洞 196 个（占 63%），其中互联网上出现“Appneta Tcpreplay 缓冲区溢出漏洞、Pimcore SQL 注入漏洞（CNVD-2022-29569）”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 4626 个，与上周（3611 个）环比增加 28%。

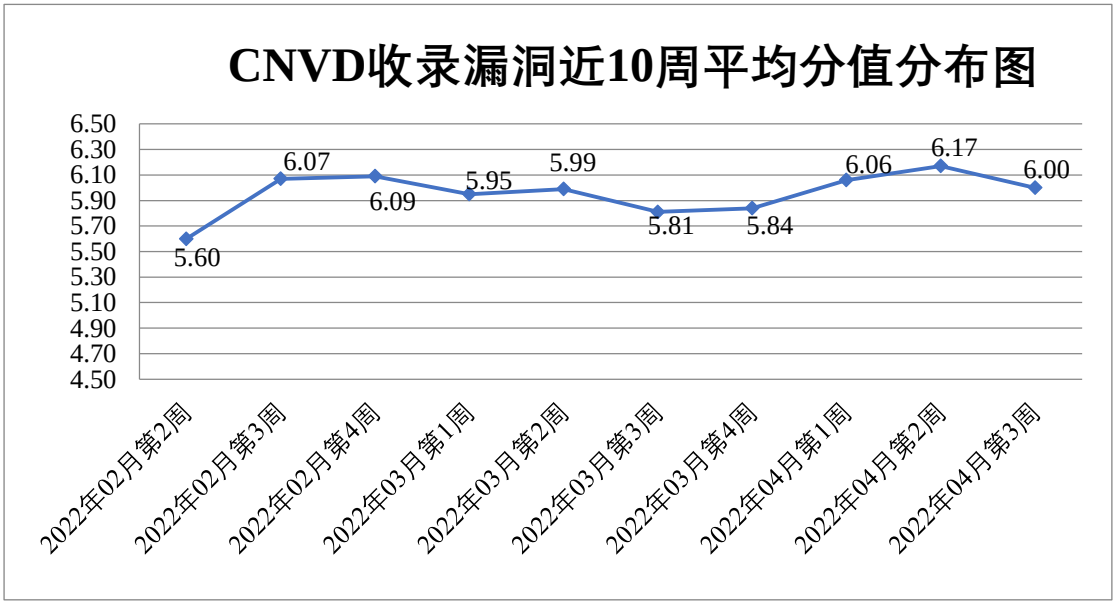

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 48 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 1778 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 122 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 120 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：

淄博闪灵网络科技有限公司、珠海新华通软件股份有限公司、珠海金山办公软件有限公司、重庆远秋科技有限公司、正方软件股份有限公司、浙江深大智能科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、长沙米拓信息技术有限公司、长沙德尚网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、易时代新图软件有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、小米科技有限责任公司、夏普商贸（中国）有限公司、西安九佳易信息资讯有限公司、西安菜瓜云信息科技有限公司、西安佰联网络技术有限公司、武汉类森科技有限公司、温州互引信息技术有限公司、微软（中国）有限公司、网新科技集团有限公司、通用电气（GE）公司、腾亿网络科技有限公司、太原迅易科技有限公司、苏州万户网络科技有限公司、苏州科达科技股份有限公司、四平市九州易通科技有限公司、四川蜀天梦图数据科技有限公司、思科系统（中国）网络技术有限公司、深圳英飞拓科技股份有限公司、深圳维盟科技股份有限公司、深圳市迅捷通信技术有限公司、深圳市信锐网科技术有限公司、深圳市美科星通信技术有限公司、深圳市吉祥腾达科技有限公司、深圳市多度科技有限公司、深圳市博思高科技有限公司、深圳市必联电子有限公司、深圳前海微众银行股份有限公司、深圳华视美达信息技术有限公司、深圳和新科技有限公司、上海卓卓网络科技有限公司、上海新朋程信息科技有限公司、上海声阅智能科技有限公司、上海商派网络科技有限公司、上海梦之路数字科技有限公司、上海肯特仪表股份有限公司、上海华测导航技术股份有限公司、上海孚盟软件有限公司、上海酆泽信息技术有限公司、上海泛微网络科技股份有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、山东金钟科技集团股份有限公司、厦门四信通信科技有限公司、厦门海豹他趣信息技术股份有限公司、三星（中国）投资有限公司、润申信息科技（上海）有限公司、青岛自动化仪表有限公司、青岛易软天创网络科技有限公司、麒麟软件有限公司、普联技术有限公司、迈普通信技术股份有限公司、灵宝简好网络科技有限公司、敬业钢铁有限公司、江苏曼荼罗软件股份有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南建研信息技术股份有限公司、黑龙江立高科技股份有限公司、河北先河环保科技股份有限公司、河北白晶环境科技有限公司、杭州益仕行信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州迪普科技股份有限公司、海南赞赞网络科技有限公司、广州易东信息安全技术有限公司、广州图创计算机软件开发有限公司、广州市保伦电子有限公司、广州红帆科技有限公司、广联达科技股份有限公司、广东盈世计算机科技有限公司、广东拓迪智

能科技有限公司、高德软件有限公司、富士胶片商业创新（中国）有限公司、福建鑫诺医疗股份有限公司、福建方维信息科技有限公司、东华医为科技有限公司、东莞市智跃软件科技有限公司、东莞市冬惊鱼网络科技有限公司、帝兴软件开发有限公司、成都星锐蓝海网络科技有限公司、成都万江港利科技有限公司、北京易聊科技有限公司、北京亿信华辰软件有限责任公司、北京星网锐捷网络技术有限公司、北京五指互联科技有限公司、北京通达信科科技有限公司、北京神州视翰科技有限公司、北京清元优软科技有限公司、北京派网软件有限公司、北京谋智火狐信息技术有限公司、北京灵州网络技术有限公司、北京猎鹰安全科技有限公司、北京九思协同软件有限公司、北京京东叁佰陆拾度电子商务有限公司、北京金和网络股份有限公司、北京东华万兴软件有限公司、安科瑞电气股份有限公司、安徽旭帆信息科技有限公司、安徽省科大奥锐科技有限公司、安徽科迅教育装备集团有限公司、阿里巴巴集团安全应急响应中心、百度安全应急响应中心、简单 CMS、熊海 CMS、信呼、小 z 博客、Yeelight、worldeyecam、WEAVEWORKS、The Apache Software Foundation、TaoCMS、Sonatype、Solar monitor、SEACMS、phpMyAdmin、Oracle、NETGEAR、mySCADA Technologies、Mlflow、Ivanti、HashiCorp、Glyph & Cog, LLC、Geovision、fibergate、emlog、Dreamer CMS、DaiCuo、CODESYS Group、Alpha Technologies、ABB 集团。

本周，CNVD 发布了《Microsoft 发布 2022 年 4 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7601

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、新华三技术有限公司、杭州安恒信息技术股份有限公司、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等单位报送公开收集的漏洞数量较多。重庆都会信息科技有限公司、杭州海康威视数字技术股份有限公司、杭州默安科技有限公司、贵州泰若数字科技有限公司、内蒙古洞明科技有限公司、北京山石网科信息技术有限公司、长春嘉诚信息技术股份有限公司、上海纽盾科技股份有限公司、广州百蕴启辰科技有限公司、河南东方云盾信息技术有限公司、任子行网络技术股份有限公司、浙江大学控制科学与工程学院、杭州美创科技有限公司、北方实验室（沈阳）股份有限公司、北京威努特技术有限公司、广西等保安全测评有限公司、武汉安域信息安全技术有限公司、河南灵创电子科技有限公司、墨菲未来科技（北京）有限公司、河南信安世纪科技有限公司、广东蓝爵网络安全技术股份有限公司、北京远禾科技有限公司、海南神州希望网络有限公司、上海上讯信息技术股份有限公司、快页信息技术有限公司、北京机沃科技有限公司、广西塔易信息技术有限公司、江苏保旺达软件技术有限公司、山石网科通信技术股份有限公司、北京冠程

科技有限公司、河南金盾信安检测评估中心有限公司、河北华测信息技术有限公司及其他个人白帽子向 CNVD 提交了 4626 个以事件型漏洞为主的原创漏洞，其中包括上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 1712 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
上海交大	1150	1150
深信服科技股份有限公司	1035	0
奇安信网神（补天平台）	562	562
新华三技术有限公司	436	0
杭州安恒信息技术股份有限公司	310	61
三六零数字安全科技集团有限公司	274	0
安天科技集团股份有限公司	216	0
北京天融信网络安全技术有限公司	214	14
阿里云计算有限公司	200	0
北京神州绿盟科技有限公司	193	13
远江盛邦（北京）网络安全科技股份有限公司	138	138
恒安嘉新（北京）科技股份公司	92	0
西安四叶草信息技术有限公司	83	83
北京启明星辰信息安全技术有限公司	77	18
北京数字观星科技有限公司	61	0
内蒙古云科数据服务股份有限公司	51	51

天津市国瑞数码安全系统股份有限公司	51	0
京东科技信息技术有限公司	41	41
中国电信集团系统集成有限责任公司	23	0
杭州迪普科技股份有限公司	15	0
南京联成科技发展股份有限公司	8	8
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京华顺信安科技有限公司	213	0
重庆都会信息科技有限公司	125	125
杭州海康威视数字技术股份有限公司	81	81
亚信科技（成都）有限公司	70	0
杭州默安科技有限公司	43	43
贵州泰若数字科技有限公司	33	33
西门子（中国）有限公司	26	0
内蒙古洞明科技有限公司	25	25
北京山石网科信息技术有限公司	17	17
长春嘉诚信息技术股份有限公司	13	13
上海纽盾科技股份有限公司	7	7

广州百蕴启辰科技有限公司	7	7
河南东方云盾信息技术有限公司	6	6
任子行网络技术股份有限公司	5	5
浙江大学控制科学与工程学院	4	4
杭州美创科技有限公司	3	3
北方实验室（沈阳）股份有限公司	2	2
北京威努特技术有限公司	2	2
广西等保安全测评有限公司	2	2
武汉安域信息安全技术有限公司	2	2
河南灵创电子科技有限公司	2	2
墨菲未来科技（北京）有限公司	1	1
河南信安世纪科技有限公司	1	1
广东蓝爵网络安全技术股份有限公司	1	1
北京远禾科技有限公司	1	1
海南神州希望网络有限公司	1	1
上海上讯信息技术股份有限公司	1	1
快页信息技术有限公司	1	1
北京机沃科技有限公	1	1

司		
广西塔易信息技术有限公司	1	1
江苏保旺达软件技术有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京冠程科技有限公司	1	1
河南金盾信安检测评估中心有限公司	1	1
河北华测信息技术有限公司	1	1
CNCERT 贵州分中心	2	2
CNCERT 浙江分中心	1	1
CNCERT 河北分中心	1	1
个人	2089	2089
报送总计	8026	4626

本周漏洞按类型和厂商统计

本周，CNVD 收录了 311 个漏洞。WEB 应用 114 个，应用程序 83 个，网络设备（交换机、路由器等网络端设备）55 个，操作系统 30 个，智能设备（物联网终端设备）26 个，数据库 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
WEB 应用	114
应用程序	83
网络设备（交换机、路由器等网络端设备）	55
操作系统	30
智能设备（物联网终端设备）	26
数据库	3

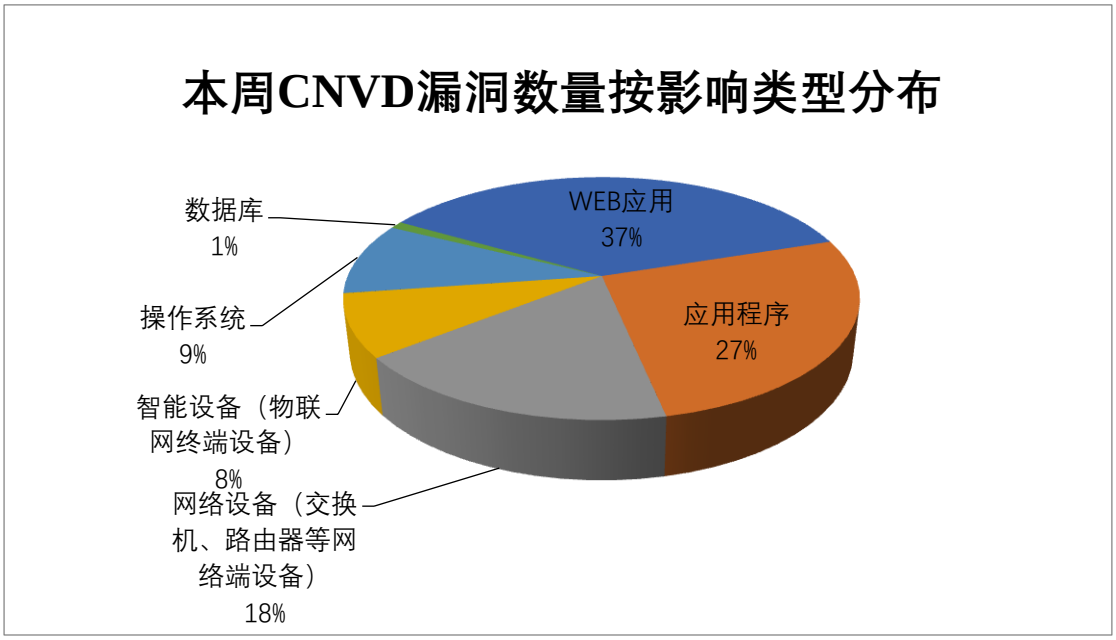

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Google、WordPress 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	25	8%
2	Siemens	25	8%
3	WordPress	14	4%
4	Microsoft	13	4%
5	Cisco	11	3%
6	Delta Electronics	8	3%
7	Open-Xchange	8	3%
8	北京星网锐捷网络技术有限公司	8	3%
9	廊坊市极致网络科技有限公司	7	2%
10	其他	192	62%

本周行业漏洞收录情况

本周，CNVD 收录了 27 个电信行业漏洞，27 个移动互联网行业漏洞，21 个工控行业漏洞（如下图所示）。其中，“Google Android 权限提升漏洞（CNVD-2022-28921）、Siemens SIMATIC Energy Manager 访问控制错误漏洞”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/

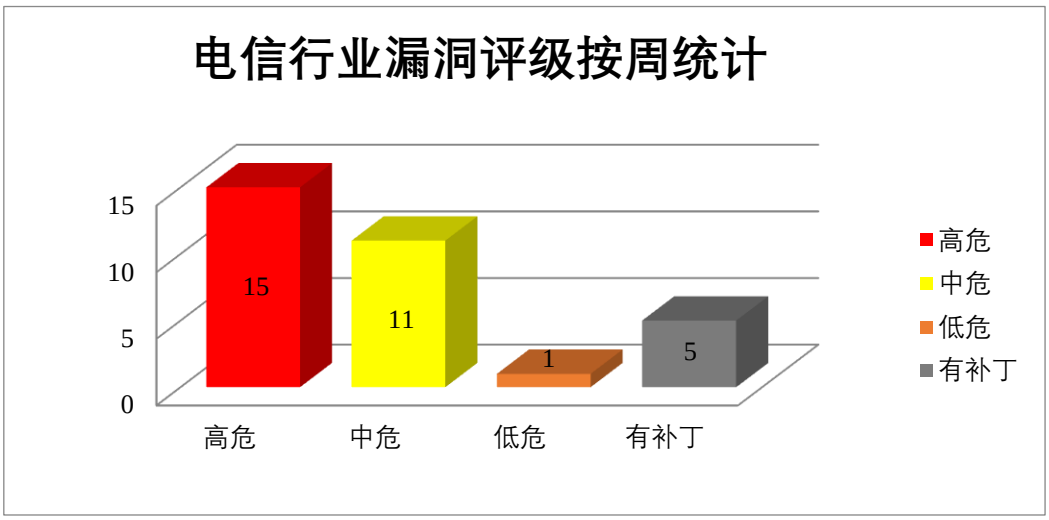

图 3 电信行业漏洞统计

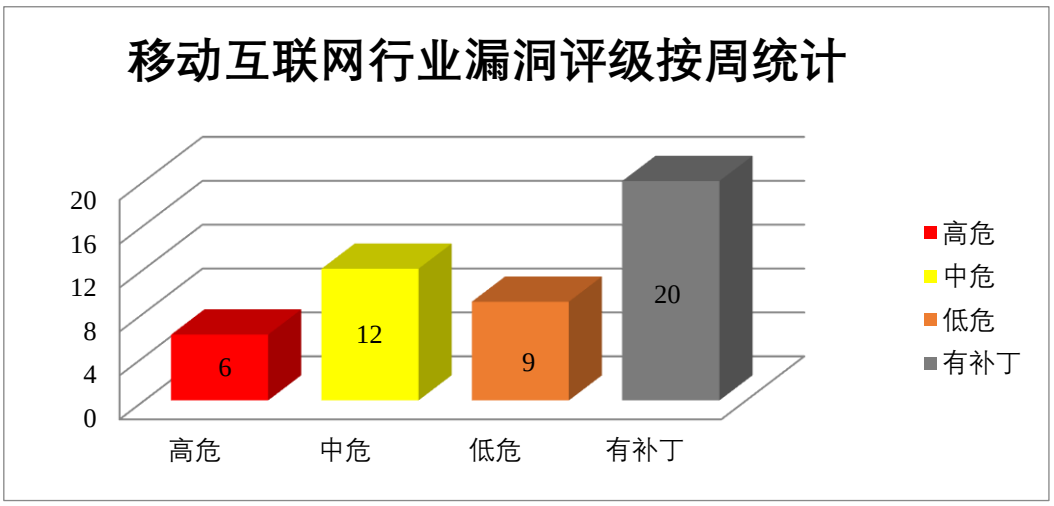

图 4 移动互联网行业漏洞统计

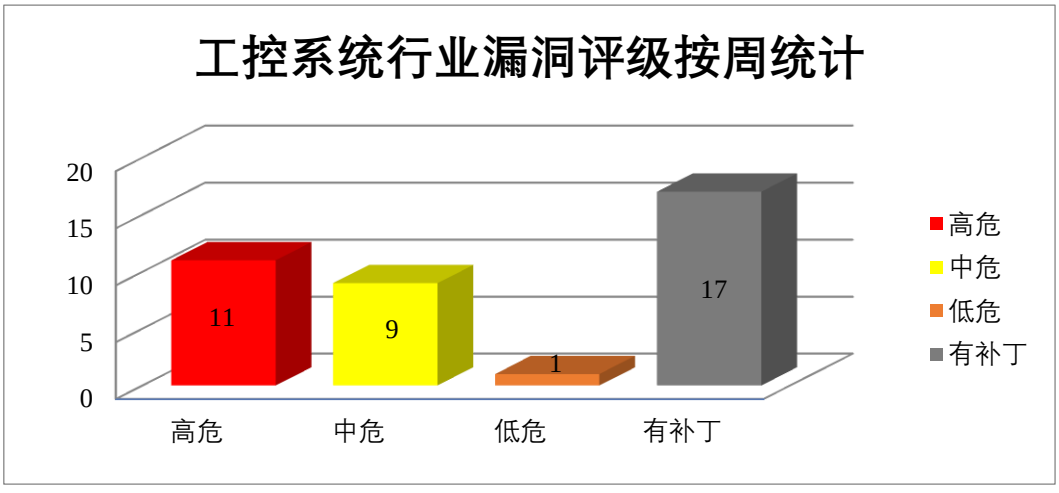

图 5 工控系统行业漏洞统计

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、 WordPress 产品安全漏洞

WordPress 是 Wordpress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在客户端执行 JavaScript 代码，上传任意文件，窃取数据库敏感数据等。

CNVD 收录的相关漏洞包括：WordPress 插件授权问题漏洞、WordPress Social Sharing plugin 跨站脚本漏洞、WordPress Popup Like box plugin 跨站脚本漏洞、WordPress Pz-LinkCard plugin 跨站脚本漏洞、WordPress Sermon Browser plugin 跨站请求伪造漏洞、WordPress Plezi plugin 跨站脚本漏洞、WordPress Popup Builder plugin SQL 注入漏洞、WordPress Narnoo Distributor plugin 路径遍历漏洞。其中，“WordPress Popup Builder plugin SQL 注入漏洞”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-2022-28801

https://www.cnvd.org.cn/flaw/show/CNVD-2022-29855

https://www.cnvd.org.cn/flaw/show/CNVD-2022-29858

https://www.cnvd.org.cn/flaw/show/CNVD-2022-29857

https://www.cnvd.org.cn/flaw/show/CNVD-2022-29856

https://www.cnvd.org.cn/flaw/show/CNVD-2022-29860

https://www.cnvd.org.cn/flaw/show/CNVD-2022-29859

https://www.cnvd.org.cn/flaw/show/CNVD-2022-29862

2、 Siemens 产品安全漏洞

SCALANCE X switches 用于连接可编程逻辑控制器等工业组件(PLC)或人机界面(HMI)。SIPLUS extreme 专为在极端条件下可靠运行而设计。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。SIMATIC PCS neo 是一种分布式控制系统 (DCS)。TIA Administrator 是一个基于 Web 的框架。Siemens Network Planner (SINETPLAN) 支持您作为基于 PROFINET 的自动化系统的规划者。TIA Portal 是一款 PC 软件。SIMATIC S7-400 CPU 系列产品专为工业环境中的过程控制而设计。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在设备上执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens SCALANCE X-300 Switch Family Devices 缓冲区溢出漏洞（CNVD-2022-28480、CNVD-2022-28484、CNVD-2022-28479）、Siemens SCALANCE X-300 Switch Family Devices 跨站请求伪造漏洞、Siemens Simcent

er Femap 存在越界写入漏洞（CNVD-2022-28488）、Siemens TIA Administrator 拒绝服务漏洞、Siemens Simcenter Femap 越界读取漏洞（CNVD-2022-28490）、Siemens SIMATIC S7-400 CPU 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-2022-28480
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28479
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28484
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28483
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28488
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28491
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28490
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28495

3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Android 是一套以 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，攻击者可利用漏洞在系统上执行任意代码或造成拒绝服务情况，提升权限等。

CNVD 收录的相关漏洞包括：Google Chrome V8 代码执行漏洞（CNVD-2022-28467）、Google Chrome File System API 信息泄露漏洞、Google Android 权限提升漏洞（CNVD-2022-28909、CNVD-2022-28911、CNVD-2022-28910、CNVD-2022-28917、CNVD-2022-28915、CNVD-2022-28918）。其中，除“Google Android 权限提升漏洞（CNVD-2022-28917、CNVD-2022-28915、CNVD-2022-28918）”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-2022-28467
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28466
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28909
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28911
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28910
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28917
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28915
https://www.cnvd.org.cn/flaw/show/CNVD-2022-28918

4、Microsoft 产品安全漏洞

Microsoft Windows 是一款由美国微软公司开发的窗口化操作系统。Microsoft Office 是一款办公软件套件产品。该产品常用组件包括 Word、Excel、Access、Powerpoint、

FrontPage 等。Microsoft SharePoint 是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。Microsoft Visual Studio Code 是一款开源的代码编辑器。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、提升权限等。

CNVD 收录的相关漏洞包括：Microsoft Windows Win32k 权限提升漏洞（CNVD-2022-29559、CNVD-2022-29560）、Microsoft Windows Telephony Server 权限提升漏洞（CNVD-2022-29562）、Microsoft Windows Upgrade Assistant 远程代码执行漏洞（CNVD-2022-29561）、Microsoft Office 远程代码执行漏洞（CNVD-2022-29564）、Microsoft Windows Kernel 信息泄露漏洞（CNVD-2022-29563）、Microsoft SharePoint Server 欺骗漏洞（CNVD-2022-29567）、Microsoft Visual Studio Code 代码注入漏洞（CNVD-2022-29568）。其中，“Microsoft Windows Win32k 权限提升漏洞（CNVD-2022-29559、CNVD-2022-29560）、Microsoft Office 远程代码执行漏洞（CNVD-2022-29564）”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-2022-29559
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29562
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29561
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29560
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29564
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29563
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29567
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29568

5、Linux kernel 缓冲区溢出漏洞（CNVD-2022-29295）

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 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞绕过 Linux 内核的访问限制，通过特定内容来读取或修改数据。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-2022-29295

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-2022-27555	Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2022-27555）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.deltaww.com/en-US/ind

			ex
CNVD-2022-27558	Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2022-27558）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.deltaww.com/en-US/index
CNVD-2022-28477	NETGEAR EX6100v1 堆栈溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://kb.netgear.com/000064615/Security-Advisory-for-Pre-Authentication-Command-Injection-on-EX6100v1-and-Pre-Authentication-Stack-Overflow-on-Multiple-Products-PSV-2021-0282-PSV-2021-0288
CNVD-2022-28492	Siemens SIMATIC Energy Manager 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://www.siemens.com
CNVD-2022-29565	Adobe Photoshop 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://helpx.adobe.com/security/products/photoshop/apsb22-20.html
CNVD-2022-29579	OTRS 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://otrs.com/release-notes/otrs-security-advisory-2022-03/
CNVD-2022-29585	Calibre-Web 存在服务器端跨站请求伪造漏洞（CNVD-2022-29585）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/janeczku/calibre-web/commit/965352c8d96c9eae7a6867ff76b0db137d04b0b8
CNVD-2022-29583	Veeam Backup&Replication 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.veeam.com/kb4290
CNVD-2022-29582	Veeam Backup&Replication 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.veeam.com/kb4290
CNVD-2022-29586	Calibre-Web 服务器端跨站请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/janeczku/calibre-web/commit/965352c8d96c9eae7a6867ff76b0db137d04b0b8

小结：本周，WordPress 产品被披露存在多个漏洞，攻击者可利用漏洞在客户端执行 JavaScript 代码，上传任意文件，窃取数据库敏感数据等。此外，Siemens、Google、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码，

提升权限导致拒绝服务等。另外，Linux kernel 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞绕过 Linux 内核的访问限制，通过特定内容来读取或修改数据。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、Pimcore SQL 注入漏洞（CNVD-2022-29569）

验证描述

Pimcore 是奥地利 Pimcore 公司的一套开源的用于创建和管理 Web 应用程序的 Web 内容管理平台。该平台集成了 Web 内容管理、电子商务框架和产品信息管理等应用。

Pimcore 10.3.5 之前版本存在 SQL 注入漏洞，该漏洞源于 ElementController.php 缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://huntr.dev/bounties/ae8dc737-844e-40da-a9f7-e72d8e50f6f9/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-29569

信息提供者

新华三技术有限公司

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. 谷歌浏览器更新，修复一零日漏洞

谷歌发布了适用于 Windows、Mac 和 Linux 的更新版本 Chrome 100.0.4896.127，又修复一零日漏洞 CVE-2022-1364，即 Chrome V8 JavaScript 引擎中一个高危类型混淆漏洞。

参考链接：https://www.freebuf.com/news/329068.html

2. 思科修复身份验证绕过漏洞

思科无线局域网控制器软件中存在高危漏洞，攻击者能够利用该漏洞绕过身份验证控制并通过管理界面登录设备，以控制受影响的系统。目前，Cisco 已经发布了安全更新。

参考链接：https://www.freebuf.com/news/329230.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