国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 12 月 26 日-2023 年 01 月 01 日　　2022 年第 52 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 474 个，其中高危漏洞 215 个、中危漏洞 228 个、低危漏洞 31 个。漏洞平均分值为 6.45。本周收录的漏洞中，涉及 0day 漏洞 341 个（占 72%），其中互联网上出现“Etaplighting Etap Safety Manager 跨站脚本漏洞、Food Ordering Management System 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 47744 个，与上周（36292 个）环比增加 32%。

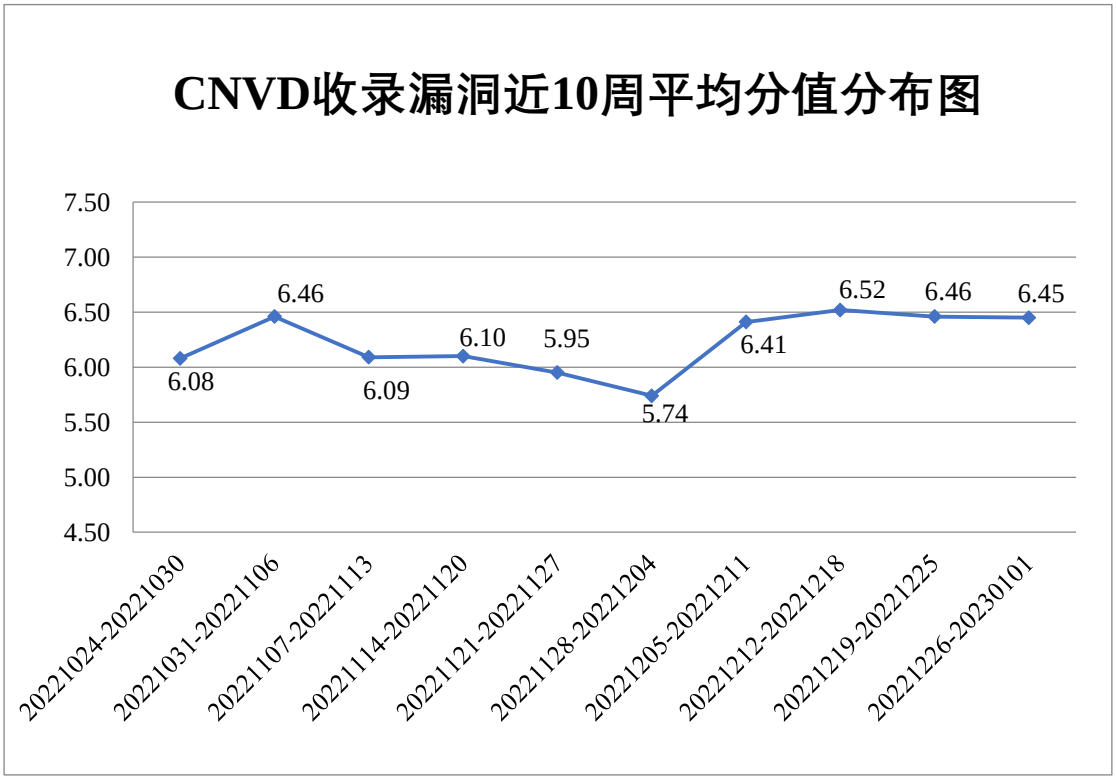

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 42 起，向基础电信企业通报漏洞事件 43 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 659 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 121 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 96 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：

浙江正元智慧科技股份有限公司、浙江浙大中控信息技术有限公司、浙江维尔科技有限公司、浙江淘宝网络有限公司、浙江波星通卫星通信有限公司、掌如科技服务有限公司、长沙翱云网络科技有限公司、云南滇约出行科技有限公司、兄弟（中国）商业有限公司、新浪网技术（中国）有限公司、携程旅行网、西安博冠教育科技有限公司、武汉天地伟业科技有限公司、无锡信捷电气股份有限公司、天地伟业技术有限公司、汤臣倍健股份有限公司、随锐科技集团股份有限公司、苏州必捷网络有限公司、四川明腾信息技术有限公司、水月居科技有限公司、深圳智慧光迅信息技术有限公司、深圳市思迅软件股份有限公司、深圳市尼高企业形象设计有限公司、深圳市绿联科技股份有限公司、深圳市捷视飞通科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳市皓峰通讯技术有限公司、深圳市大世同舟信息科技有限公司、深圳市百为通达科技有限公司、深圳华视美达信息技术有限公司、深圳邦健生物医疗设备股份有限公司、上海卓卓网络科技有限公司、上海三瑞信息技术有限公司、上海赛连信息科技有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海楚果信息技术有限公司、商派软件有限公司、山脉科技股份有限公司、山东金钟科技集团股份有限公司、山东国子软件股份有限公司、厦门四信通信科技有限公司、厦门城中城商业管理有限公司、启明信息技术股份有限公司、南京骏飞科技有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、洪湖尔创网联信息技术有限公司、黑龙江越久科技有限公司、河北鑫考教育科技股份有限公司、河北蓝蜂信息科技有限公司、合肥市道克莱尔信息科技有限公司、杭州雄伟科技开发股份有限公司、杭州思福迪信息技术有限公司、杭州乐湾科技有限公司、杭州瀚洋科技有限公司、广州优胜特软件开发有限公司、广州市保伦电子有限公司、广州锦铭泰软件科技有限公司、广西南宁领众网络科技有限公司、福州联迅信息科技有限公司、福建亿能达信息技术股份有限公司、帝国软件、道尔大数据科技有限公司、大连华天软件有限公司、成都飞鱼星科技股份有限公司、北京优炫软件股份有限公司、北京星网锐捷网络技术有限公司、北京网御星云信息技术有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京派网软件有限公司、北京金和网络股份有限公司、北京传奇华

育教育科技股份有限公司、北京百卓网络技术有限公司、百度安全应急响应中心、安吉加加信息技术有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心和Lexmark。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，杭州安恒信息技术股份有限公司、新华三技术有限公司、北京启明星辰信息安全技术有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。贵州泰若数字科技有限公司、北京山石网科信息技术有限公司、北京安盟信息技术股份有限公司、快页信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、山东云天安全技术有限公司、重庆都会信息科技有限公司、杭州默安科技有限公司、山东新潮信息技术有限公司、博智安全科技股份有限公司、重庆易阅科技有限公司、北京网猿科技有限公司、山东九域信息技术有限公司、赛尔网络有限公司、北京华顺信安信息技术有限公司、中国电信股份有限公司网络安全产品运营中心、苏州棱镜七彩信息科技有限公司、安徽锋刃信息科技有限公司、河南悦海数安科技有限公司、北京升鑫网络科技有限公司、云南联创网安科技有限公司、山石网科通信技术股份有限公司、北京微步在线科技有限公司、中通服创发科技有限责任公司、听潮盛世（北京）科技有限公司、杭州美创科技有限公司、西安交大捷普网络科技有限公司、北京安帝科技有限公司、神州灵云（北京）科技有限公司、上海纽盾科技股份有限公司、浙江东安检测技术有限公司、南方电网数字电网研究院有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、上海齐同信息科技有限公司、河南灵创电子科技有限公司、中科国宏科技有限公司及其他个人白帽子向 CNVD 提交了 47744 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）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 45182 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
斗象科技（漏洞盒子）	32556	32556
奇安信网神（补天平台）	11420	11420
三六零数字安全科技集团有限公司	981	981
杭州安恒信息技术股份有限公司	397	365
新华三技术有限公司	391	0

北京启明星辰信息安全技术有限公司	308	2
安天科技集团股份有限公司	305	0
北京神州绿盟科技有限公司	283	0
深信服科技股份有限公司	243	0
天津市国瑞数码安全系统股份有限公司	236	0
上海交大	225	225
西安四叶草信息技术有限公司	190	190
远江盛邦（北京）网络安全科技股份有限公司	124	124
恒安嘉新（北京）科技股份公司	113	0
北京数字观星科技有限公司	111	0
京东科技信息技术有限公司	18	2
中国电信集团系统集成有限责任公司	17	0
南京众智维信息科技有限公司	15	15
北京长亭科技有限公司	9	9
北京天融信网络安全技术有限公司	5	2
南京联成科技发展股份有限公司	2	2
北京信联科汇科技有限公司	2	2
北京智游网安科技有	1	1

限公司		
北京知道创宇信息技术股份有限公司	1	0
贵州泰若数字科技有限公司	225	225
北京山石网科信息技术有限公司	166	166
北京安盟信息技术股份有限公司	52	52
快页信息技术有限公司	39	39
奇安星城网络安全运营服务（长沙）有限公司	35	35
河南东方云盾信息技术有限公司	34	34
山东云天安全技术有限公司	30	30
重庆都会信息科技有限公司	27	27
杭州默安科技有限公司	24	24
山东新潮信息技术有限公司	17	17
博智安全科技股份有限公司	16	16
重庆易阅科技有限公司	12	12
北京网猿科技有限公司	9	9
山东九域信息技术有限公司	8	8
赛尔网络有限公司	8	8
北京华顺信安信息技术有限公司	7	7

中国电信股份有限公司网络安全产品运营中心	6	6
苏州棱镜七彩信息科技有限公司	5	5
安徽锋刃信息科技有限公司	4	4
河南悦海数安科技有限公司	3	3
北京升鑫网络科技有限公司	2	2
云南联创网安科技有限公司	2	2
山石网科通信技术股份有限公司	2	2
北京微步在线科技有限公司	2	2
中通服创发科技有限责任公司	1	1
听潮盛世（北京）科技有限公司	1	1
杭州美创科技有限公司	1	1
西安交大捷普网络科技有限公司	1	1
北京安帝科技有限公司	1	1
神州灵云（北京）科技有限公司	1	1
上海纽盾科技股份有限公司	1	1
浙江东安检测技术有限公司	1	1
南方电网数字电网研究院有限公司	1	1

北京云科安信科技有限公司（Seraph 安全实验室）	1	1
上海齐同信息科技有限公司	1	1
河南灵创电子科技有限公司	1	1
中科国宏科技有限公司	1	1
CNCERT 内蒙古分中心	3	3
CNCERT 甘肃分中心	1	1
个人	1096	1096
报送总计	49801	47744

本周漏洞按类型和厂商统计

本周，CNVD 收录了 474 个漏洞。WEB 应用 226 个，应用程序 92 个，网络设备（交换机、路由器等网络端设备）67 个，操作系统 57 个，智能设备（物联网终端设备）23 个，安全产品 7 个，数据库 2 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	226
应用程序	92
网络设备（交换机、路由器等网络端设备）	67
操作系统	57
智能设备（物联网终端设备）	23
安全产品	7
数据库	2

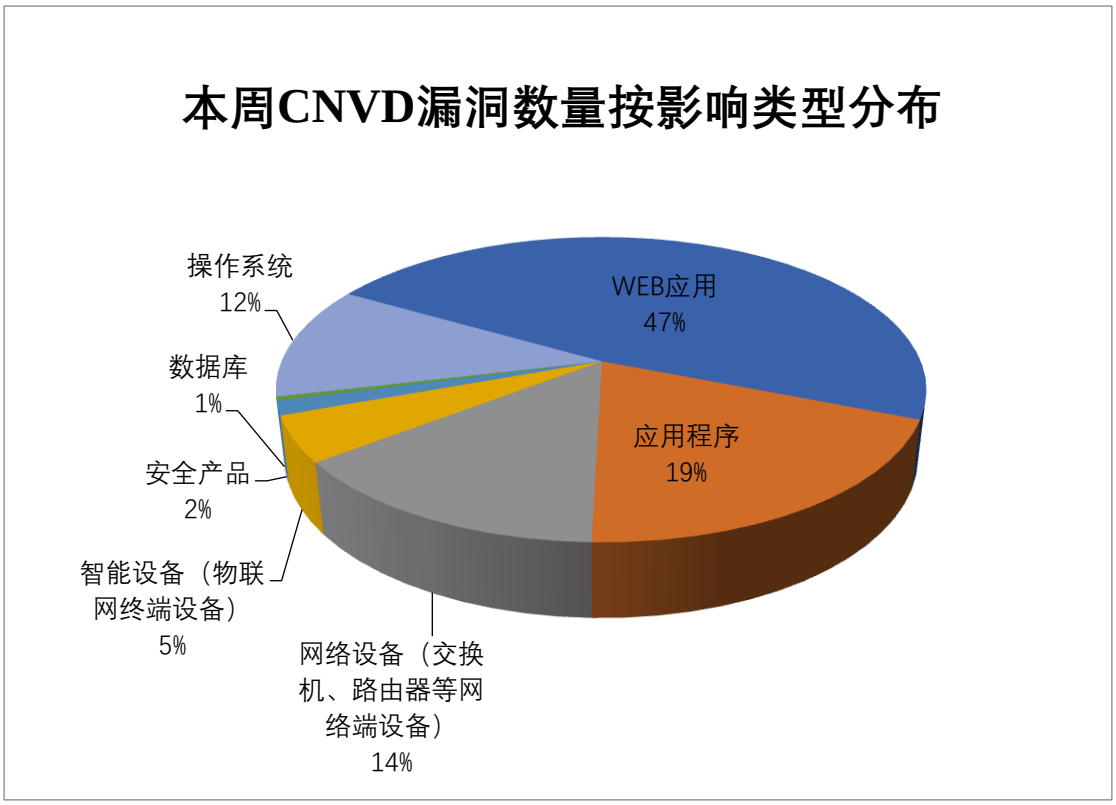

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Siemens、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	Microsoft	48	10%
2	Siemens	23	5%
3	Adobe	14	3%
4	深圳市思迅软件股份有限公司	13	3%
5	Google	12	3%
6	IBM	10	2%
7	H3C	11	2%
8	北京百卓网络技术有限公司	9	2%
9	HP	8	2%
10	其他	326	68%

本周行业漏洞收录情况

本周，CNVD 收录了 35 个电信行业漏洞，25 个移动互联网行业漏洞，22 个工控行

业漏洞（如下图所示）。其中，“Siemens LOGO! 8 BM 缓冲区溢出漏洞（CNVD-2022-89767）、Google Android 代码执行漏洞（CNVD-2022-89776）、多款 Siemens 产品输入验证错误漏洞”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/

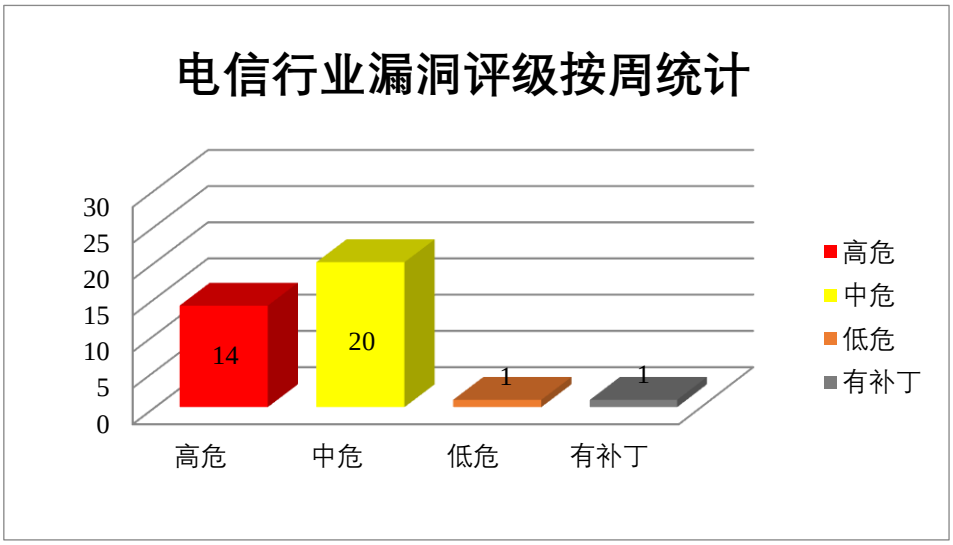

图 3 电信行业漏洞统计

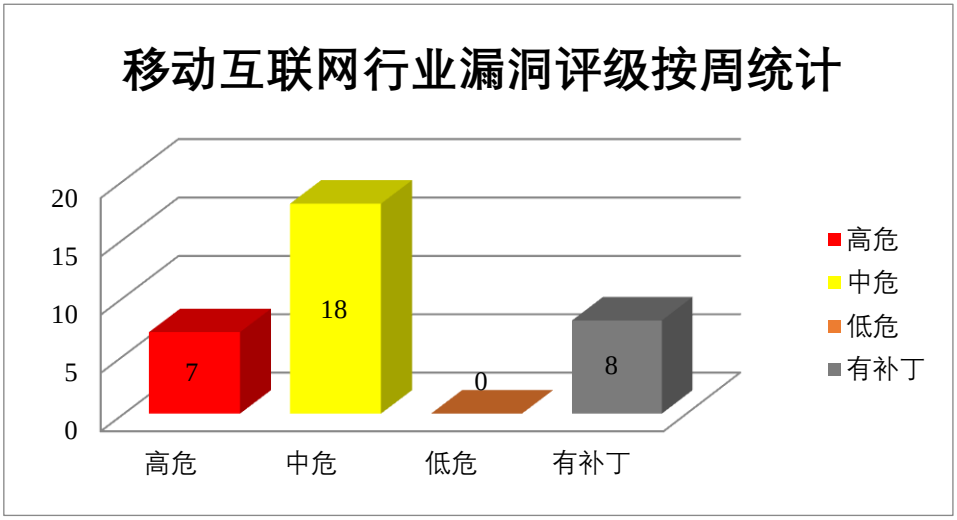

图 4 移动互联网行业漏洞统计

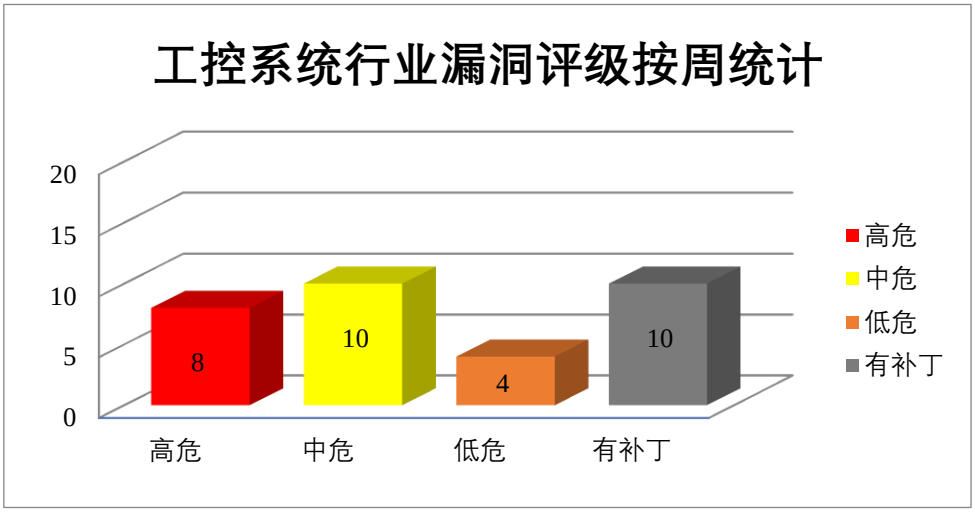

图 5 工控系统行业漏洞统计

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、 Siemens 产品安全漏洞

Siemens Parasolid 是德国西门子（Siemens）公司的一个几何建模内核。Siemens Simcenter STAR-CCM+是德国西门子（Siemens）公司的一个完整的多物理场解决方案，可对真实条件下工作的产品和设计进行仿真。Siemens SICAM PAS/PQS 是德国西门子（Siemens）公司的一款带有用于能源自动化和电能质量操作系统的软件。Siemens Solid Edge 是德国西门子（Siemens）公司的一款三维 CAD 软件。该软件可用于零件设计、装配设计、钣金设计、焊接设计等行业。Siemens LOGO! 8 BM 是德国西门子（Siemens）公司的一个用于工业环境用于 Windows 平台的编程软件。Siemens Industrial Edge Management 是德国西门子（Siemens）公司的一个平台，用于在靠近车间的计算平台上托管来自不同供应商的应用程序。Siemens Desigo PX 是德国西门子（Siemens）公司的一套楼宇自动化控制系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以 root 权限执行任意系统命令，在应用程序崩溃时发送消息并创建拒绝服务条件等。

CNVD 收录的相关漏洞包括：Siemens Parasolid 越界写入漏洞（CNVD-2022-89757）、Siemens Simcenter STAR-CCM+权限提升漏洞、Siemens SICAM PAS/PQS 输入验证错误漏洞、Siemens Solid Edge 堆缓冲区溢出漏洞（CNVD-2022-89764）、Siemens LOGO! 8 BM 输入验证错误漏洞（CNVD-2022-89766）、Siemens LOGO! 8 BM 缓冲区溢出漏洞（CNVD-2022-89767）、Siemens Industrial Edge Management 信任管理问题漏洞、多款 Siemens 产品操作系统命令注入漏洞。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-2022-89757
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89758
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89760
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89764
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89766
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89767
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91613
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91640

2、Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的一套以 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，在系统上执行任意代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-89770、CNVD-2022-89777）、Google Android 拒绝服务漏洞（CNVD-2022-89771、CNVD-2022-89772、CNVD-2022-89773）、Google Android 代码执行漏洞（CNVD-2022-89774、CNVD-2022-89776）、Google Android 信息泄露漏洞（CNVD-2022-89775）。其中，“Google Android 权限提升漏洞（CNVD-2022-89770、CNVD-2022-89777）、Google Android 代码执行漏洞（CNVD-2022-89774、CNVD-2022-89776）” 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-2022-89770
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89771
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89772
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89773
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89774
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89775
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89776
https://www.cnvd.org.cn/flaw/show/CNVD-2022-89777

3、IBM 产品安全漏洞

IBM Security Verify Governance Identity Manager 是 IBM 一款基于网络设备的集成，主要用以业务为中心的规则、活动和流程。IBM Spectrum Control（前称 Tivoli Storage Productivity Center）是美国国际商业机器（IBM）公司的一套存储资源管理软件。该软件可以为多个存储系统提供监控、自动化和分析。IBM Security Guardium 是美国国际商业机器（IBM）公司的一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。IBM Cognos Analytics 是美国 IBM 公司的一

套商业智能软件。该软件包括报表、仪表板和记分卡等，并可通过分析关键因素与关键人等内容，协助企业调整决策。IBM Engineering Requirements Quality Assistant 是美国 IBM 公司的一款基于 Watson AI 用于辅助开发人员提高工程需求质量的软件。该应用可显著降低发现缺陷成本，有利于尽早发现工程流程中的需求错误，加快产品上市。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞向内部网络或本地文件系统发出任意请求，获取敏感信息，在 Web UI 中嵌入任意 JavaScript 代码等。

CNVD 收录的相关漏洞包括：IBM Security Verify Governance Identity Manager 信息泄露漏洞（CNVD-2022-91125）、IBM Spectrum Control 弱加密漏洞、IBM Security Guardium 信息泄露漏洞（CNVD-2022-91128）、IBM Cognos Analytics 服务器端请求伪造漏洞、IBM Cognos Analytics 跨站脚本漏洞（CNVD-2022-91132）、IBM Cognos Analytics 敏感信息泄露漏洞（CNVD-2022-91131）、IBM Cognos Analytics 日志注入漏洞、IBM Engineering Requirements Quality Assistant 输入验证错误漏洞。其中，“IBM Spectrum Control 弱加密漏洞、IBM Cognos Analytics 服务器端请求伪造漏洞、IBM Cognos Analytics 日志注入漏洞”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-2022-91125
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91129
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91128
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91133
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91132
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91131
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91130
https://www.cnvd.org.cn/flaw/show/CNVD-2022-91136

4、 Adobe 产品安全漏洞

Adobe Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞在浏览器上下文中执行恶意 JavaScript。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2022-91149、CNVD-2022-91148、CNVD-2022-91147、CNVD-2022-91146、CNVD-2022-91152、CNVD-2022-91151、CNVD-2022-91150、CNVD-2022-91156）。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-2022-91149

https://www.cnvd.org.cn/flaw/show/CNVD-2022-91148

https://www.cnvd.org.cn/flaw/show/CNVD-2022-91147

https://www.cnvd.org.cn/flaw/show/CNVD-2022-91146

https://www.cnvd.org.cn/flaw/show/CNVD-2022-91152

https://www.cnvd.org.cn/flaw/show/CNVD-2022-91151

https://www.cnvd.org.cn/flaw/show/CNVD-2022-91150

https://www.cnvd.org.cn/flaw/show/CNVD-2022-91156

5、LibreNMS 命令注入漏洞（CNVD-2022-91160）

LibreNMS 是 LibreNMS 社区的一套基于 PHP 和 MySQL 的开源网络监控系统。该系统具有自定义警报、自动发现网络环境和自动更新等特点。本周，LibreNMS 被披露存在命令注入漏洞，该漏洞源于 service_ip、hostname 和 service_param 参数未能正确过滤构造命令特殊字符、命令等。攻击者可利用该漏洞导致任意命令执行。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-2022-91160

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-2022-91619	多款 Siemens 产品输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cert-portal.siemens.com/productcert/pdf/ssa-384224.pdf
CNVD-2022-91594	Google protobuf-java 拒绝服务漏洞	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/protocolbuffers/protobuf/security/advisories/GHSA-h4h5-3hr4-j3g2
CNVD-2022-91630	Microsoft Windows Group Policy 特权提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37975
CNVD-2022-91643	Cisco Catalyst 9200 Series 交换机数据伪造问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cat-verify-D4NEQA6q
CNVD-2022-91632	Microsoft Windows Local Session Manager (LSM)拒绝服	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

	务漏洞		https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37998
CNVD-2022-91646	Cisco IOS XE 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-KU9Z8kFX
CNVD-2022-91650	fwupd 信息泄露漏洞	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/fwupd/fwupd/commit/ea676855f2119e36d433fbd2ed604039f53b2091
CNVD-2022-91659	Discourse 文件上传漏洞	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/discourse/discourse/commit/b27d5626d208a22c516a0adfda7554b67b493835
CNVD-2022-91627	Microsoft Windows DWM Core Library 特权提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-37970
CNVD-2022-91647	Cisco IOS XE Wireless Controller software 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-c9800-mob-dos-342YAc6J

小结：本周，Siemens 产品被披露存在多个漏洞，攻击者可利用漏洞以 root 权限执行任意系统命令，在应用程序崩溃时发送消息并创建拒绝服务条件等。此外，Google、IBM、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞向内部网络或本地文件系统发出任意请求，获取敏感信息，提升权限，在系统上执行任意代码，造成拒绝服务等。另外，LibreNMS 被披露存在命令注入漏洞。攻击者可利用漏洞导致任意命令执行。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、Etaplighting Etap Safety Manager 跨站脚本漏洞

验证描述

ETAP Safety Manager 是一款管理系统，用户观察、配置和维护紧急照明。

Etaplighting Etap Safety Manager 1.0.0.32 版本存在跨站脚本漏洞，该漏洞源于 action 参数在返回给用户之前未正确清理，攻击者可利用该漏洞在受影响站点上下文中的用户浏览器会话中执行任意 HTML/JS 代码。

验证信息

POC 链接：https://www.gabriel.urdhr.fr/2022/02/07/selenium-standalone-server-csrf-dns-rebinding-rce/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-91652

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. Linux Kernel 被爆可远程执行代码的“关键”SMB 漏洞

安全专家近日在 Linux Kernel 中发现了一个“关键”漏洞（CVSS 评分为 9.6 分），黑客可以利用该漏洞攻击 SMB 服务器，在远程执行任意代码。这个漏洞主要发生在启用了 ksmbd 的 SMB 服务器上。

参考链接：https://www.ithome.com/0/663/510.htm

2. 谷歌智能音箱存在后门，允许黑客窥探对话

Google Home 智能音箱中的一个漏洞允许安装一个后门帐户，该帐户可用于远程控制它，并通过访问麦克风馈送将其变成一个窥探设备。

参考链接：https://www.bleepingcomputer.com/news/security/google-home-speakers-allowed-hackers-to-snoop-on-conversations/

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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国家网络安全漏洞库，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，是我国计算机网络应急处理体系中的牵头单位。

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