国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 06 月 13 日-2022 年 06 月 19 日 **2022 年第 24 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 146 个、中危漏洞 284 个、低危漏洞 44 个。漏洞平均分值为 5.93。本周收录的漏洞中，涉及 0day 漏洞 361 个（占 76%），其中互联网上出现“CSCMS Music Portal System SQL 注入漏洞、Badminton Center 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 9231 个，与上周（42217 个）环比减少 78%。

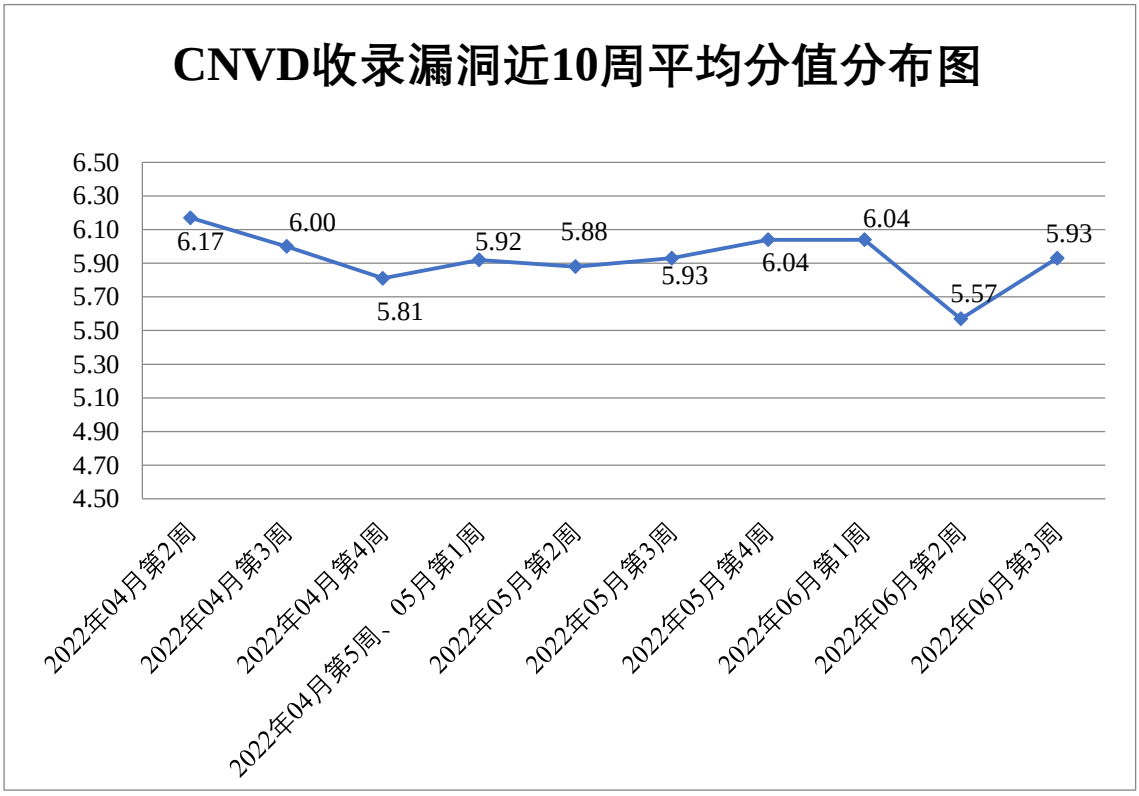

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 起，向基础电信企业通报漏洞事件 33 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 449 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 83 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 115 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：

紫光软件系统有限公司、珠海金山办公软件有限公司、中信科移动通信技术股份有限公司、中科方德软件有限公司、浙江禾匠信息科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、西门子（中国）有限公司、无锡锐泰节能系统科学有限公司、微软（中国）有限公司、天维尔信息科技股份有限公司、天津神州浩天科技有限公司、四平市九州易通科技有限公司、思科系统（中国）网络技术有限公司、深圳搜豹网络有限公司、深圳市图美电子技术有限公司、深圳市金蝶天燕云计算股份有限公司、深圳市吉祥腾达科技有限公司、深信服科技股份有限公司、上海卓卓网络科技有限公司、上海喜马拉雅科技有限公司、上海肯特仪表股份有限公司、上海黄豆网络科技有限公司、上海泛微网络科技股份有限公司、上海二三四五网络科技有限公司、上海贝锐信息科技股份有限公司、山东金钟科技集团股份有限公司、厦门三五互联科技股份有限公司、青岛东软载波智能电子有限公司、普联技术有限公司、南京康尼机电股份有限公司、明腾网络股份有限公司、昆明云涛科技有限公司、康吉诺（北京）科技有限公司、江西铭软科技有限公司、吉翁电子（深圳）有限公司、湖南省思派电子科技有限公司、湖南创星科技股份有限公司、湖南翱云网络科技有限公司、恒锋信息科技股份有限公司、杭州易软共创网络科技有限公司、汉王科技股份有限公司、海南有趣科技有限公司、广州图创计算机软件开发有限公司、广州南方卫星导航仪器有限公司、广州好象科技有限公司、广东精工智能系统有限公司、富士胶片商业创新（中国）有限公司、烽火通信科技股份有限公司、东莞市东城飞飞网络科技经营部、北京中创视讯科技有限公司、北京值得买科技股份有限公司、北京星网锐捷网络技术有限公司、北京欣泉科技有限公司、北京网康科技有限公司、北京天融信科技有限公司、北京数科网维技术有限责任公司、北京神州绿盟科技有限公司、北京巧巧时代网络科技有限公司、北京灵州网络技术有限公司、北京良精志诚科技有限责任公司、北京九思协同软件有限公司、北京汉邦高科数字技术股份有限公司、北京宝兰德软件股份有限公司、北京爱奇艺科技有限公司、三菱电机株式会社、众山小读书 APP、狂雨小说 cms、WordPress、VMware, Inc.、UCMS、StarDot Technologies、SparkPost、osCommerce、NETGEAR、Moddable、JreCms、JPress、jfinal cms、J2eeFAST、AxonIQ 和 Axis Communications AB。

本周，CNVD 发布了《Microsoft 发布 2022 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/7801

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安科技有限公司、贵州泰若数字科技有限公司、上海纽盾科技股份有限公司、重庆都会信息科技有限公司、河南东方云盾信息技术有限公司、北京安帝科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、浙江木链物联网科技有限公司、山谷网安科技股份有限公司、中科汇能科技有限公司、武汉安域信息安全技术有限公司、西安交大捷普网络科技有限公司、平安银河实验室、河南灵创电子科技有限公司、中国烟草总公司湖北省公司、广东唯顶信息科技股份有限公司、山石网科通信技术股份有限公司、北京六方云信息技术有限公司、网宿科技股份有限公司、广州百蕴启辰科技有限公司、北京墨云科技有限公司、北京机沃科技有限公司、上海嘉韦思信息技术有限公司、江苏保旺达软件技术有限公司、北京升鑫网络科技有限公司、南京凯茜数字科技有限公司及其他个人白帽子向 CNVD 提交了 9231 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）、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 7011 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
奇安信网神（补天平台）	5341	5341
斗象科技（漏洞盒子）	1315	1315
新华三技术有限公司	470	0
深信服科技股份有限公司	448	3
杭州安恒信息技术股份有限公司	437	437
北京神州绿盟科技有限公司	276	10
三六零数字安全科技集团有限公司	264	264

安天科技集团股份有限公司	224	0
北京数字观星科技有限公司	205	0
北京天融信网络安全技术有限公司	117	18
恒安嘉新（北京）科技股份公司	103	0
上海交大	91	91
北京启明星辰信息安全技术有限公司	75	16
天津市国瑞数码安全系统股份有限公司	60	0
中国电信集团系统集成有限责任公司	25	1
京东科技信息技术有限公司	23	23
内蒙古云科数据服务股份有限公司	12	12
西安四叶草信息技术有限公司	11	11
远江盛邦（北京）网络安全科技股份有限公司	6	6
北京知道创宇信息技术股份有限公司	4	0
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	119	6
贵州泰若数字科技有限公司	81	81
西门子（中国）有限公司	44	0

上海纽盾科技股份有限公司	39	39
杭州迪普科技股份有限公司	14	0
重庆都会信息科技有限公司	13	13
河南东方云盾信息技术有限公司	8	8
北京安帝科技有限公司	6	6
北京云科安信科技有限公司（Seraph 安全实验室）	4	4
浙江木链物联网科技有限公司	4	4
山谷网安科技股份有限公司	4	4
中科汇能科技有限公司	4	4
武汉安域信息安全技术有限公司	4	4
西安交大捷普网络科技有限公司	3	3
平安银河实验室	3	3
河南灵创电子科技有限公司	3	3
中国烟草总公司湖北省公司	3	3
广东唯顶信息科技股份有限公司	2	2
山石网科通信技术股份有限公司	2	2
北京六方云信息技术有限公司	1	1
网宿科技股份有限公	1	1

司		
广州百蕴启辰科技有限公司	1	1
北京墨云科技有限公司	1	1
北京机沃科技有限公司	1	1
上海嘉韦思信息技术有限公司	1	1
江苏保旺达软件技术有限公司	1	1
北京升鑫网络科技有限公司	1	1
南京凯茜数字科技有限公司	1	1
个人	1484	1484
报送总计	11361	9231

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 223 个，应用程序 120 个，网络设备（交换机、路由器等网络端设备）77 个，智能设备（物联网终端设备）21 个，安全产品 16 个，操作系统 16 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
WEB 应用	223
应用程序	120
网络设备（交换机、路由器等网络端设备）	77
智能设备（物联网终端设备）	21
安全产品	16
操作系统	16
数据库	1

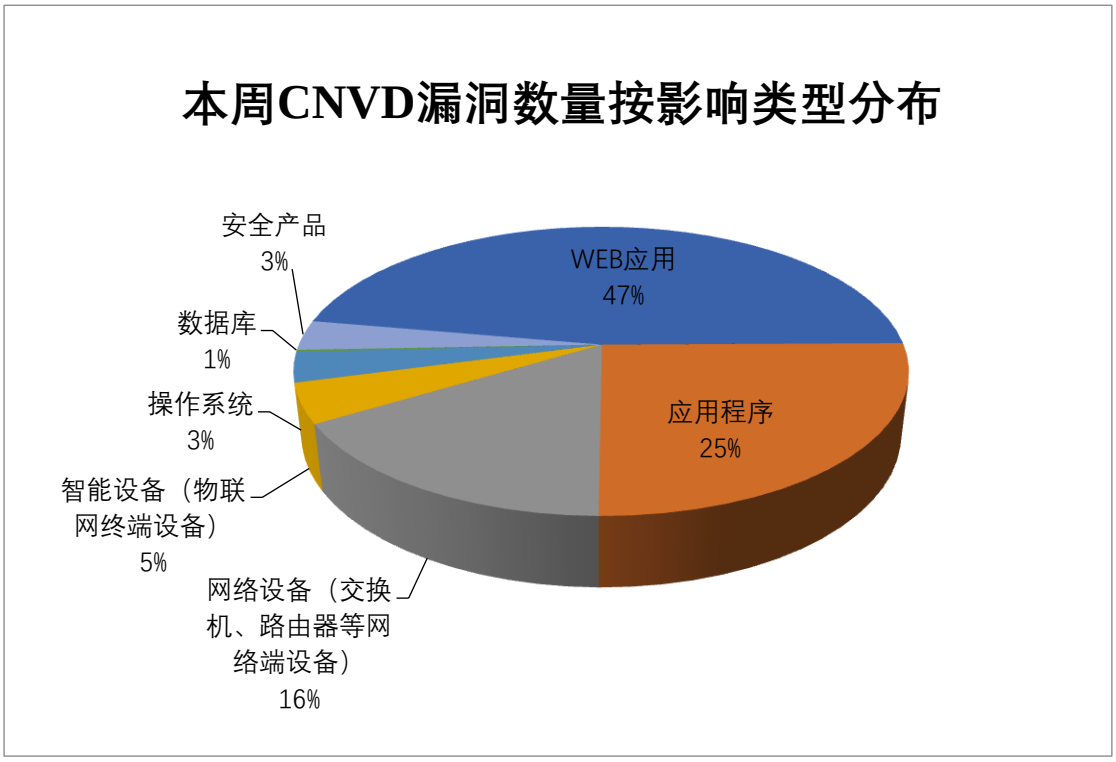

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、WordPress、Siemens 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	28	6%
2	WordPress	28	6%
3	Siemens	27	6%
4	Carlo Montero	20	4%
5	CSCMS	20	4%
6	VIM	12	3%
7	Cisco	11	2%
8	Adobe	10	2%
9	TOTOLINK	9	2%
10	其他	309	65%

本周行业漏洞收录情况

本周，CNVD 收录了 61 个电信行业漏洞，15 个移动互联网行业漏洞，26 个工控行业漏洞（如下图所示）。其中，“H3C Magic R100 缓冲区溢出漏洞、Cisco Unified CM 和 Unified CM SME 任意文件写入漏洞、Siemens SINEMA Remote Connect Server 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/

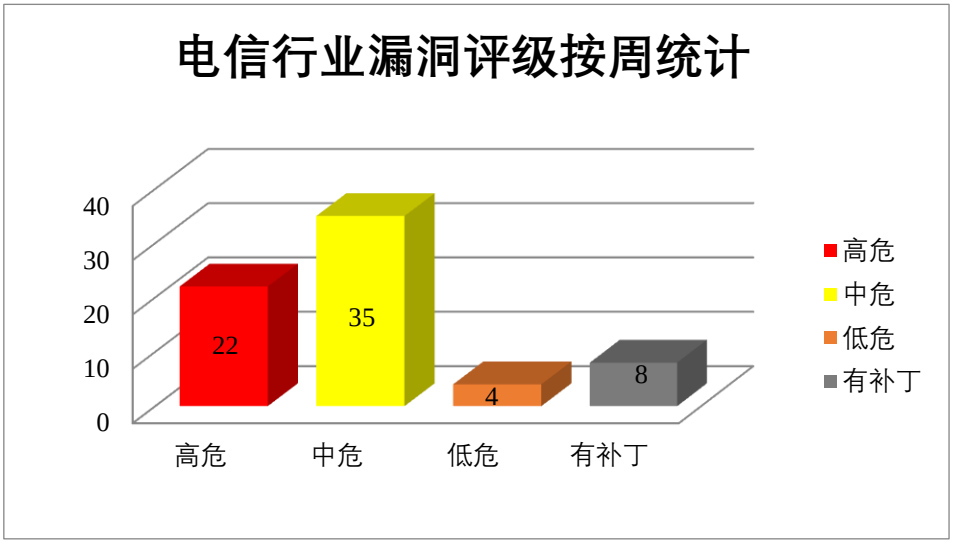

图 3 电信行业漏洞统计

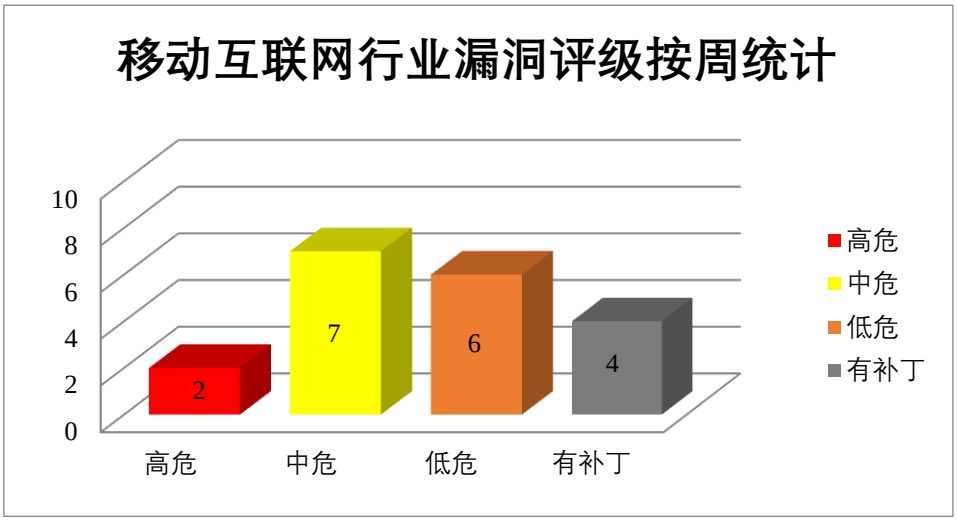

图 4 移动互联网行业漏洞统计

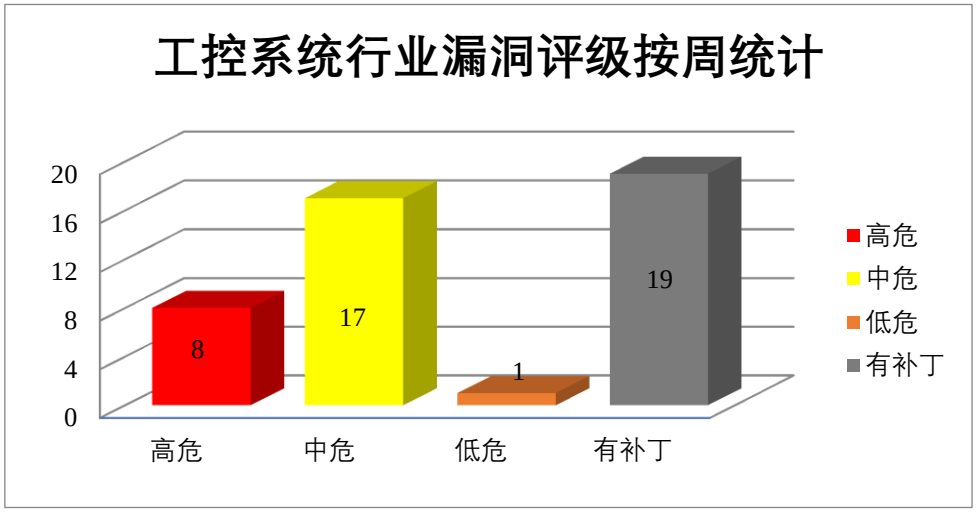

图 5 工控系统行业漏洞统计

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 Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Acrobat Reader 是一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe InCopy 是美国 Adobe 公司的一款用于创作的文本编辑软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取系统上的敏感信息，在目标系统上执行任意代码。

CNVD 收录的相关漏洞包括：多款 Adobe 产品越界读取漏洞（CNVD-2022-45905、CNVD-2022-45904、CNVD-2022-45906、CNVD-2022-45908、CNVD-2022-45907、CNVD-2022-45910、CNVD-2022-45911）、Adobe InCopy 越界写入漏洞（CNVD-2022-45913）。其中，“多款 Adobe 产品越界读取漏洞（CNVD-2022-45906）、Adobe InCopy 越界写入漏洞（CNVD-2022-45913）”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-2022-45905

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45904

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45906

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45908

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45907

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45910

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45911

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45913

2、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 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Bootloader 是其中的一个启动加载程序。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设计的 HTML 页面执行沙盒逃逸，导致权限提升，造成应用拒绝服务等。

CNVD 收录的相关漏洞包括：Google Chrome 资源管理错误漏洞（CNVD-2022-44716、CNVD-2022-44715、CNVD-2022-44718、CNVD-2022-44717、CNVD-2022-44720、CNVD-2022-44719）、Google Android 拒绝服务漏洞（CNVD-2022-45914）、Google Android 权限提升漏洞（CNVD-2022-45915）。其中，“Google Android 权限提升漏洞（CNVD-2022-45915）”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-2022-44716

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44715

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44718

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44717

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44720

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44719

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45914

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45915

3、Cisco 产品安全漏洞

Cisco Firepower Threat Defense 是一套提供下一代防火墙服务的统一软件。Cisco Adaptive Security Appliances Software 是一套防火墙和网络安全平台。该平台提供了对数据和网络资源的高度安全的访问等功能。Cisco Unified Communications Manager 是美国思科（Cisco）公司的一款统一通信系统中的呼叫处理组件。该组件提供了一种可扩展、可分布和高可用的企业 IP 电话呼叫处理解决方案。Unified Communications Manager Session Management Edition 是 Unified Communications Manager 的会话管理版。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底层操作系统上的敏感文件，执行任意脚本代码，造成拒绝服务条件（DoS）等。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliance 和 Firepower Threat Defense 信息泄露漏洞、Cisco Adaptive Security Appliance 和 Firepower Threat Defense 拒绝服务漏洞（CNVD-2022-44686、CNVD-2022-44689）、Cisco Adaptive Security Appliance 和 Firepower Threat Defense 权限提升漏洞、Cisco Unified CM 和 Unified CM SME 任意文件读取漏洞、Cisco Unified CM 和 Unified CM SME 任意文件写入漏洞、Cisco Unified CM 和 Unified CM SME 跨站脚本漏洞、Cisco Unified CM 和 Unified CM SME 拒绝服务漏洞。其中，“Cisco Adaptive Security Appliance 和 Firepower

Threat Defense 拒绝服务漏洞（CNVD-2022-44686、CNVD-2022-44689）、Cisco Adaptive Security Appliance 和 Firepower Threat Defense 权限提升漏洞、Cisco Unified CM 和 Unified CM SME 任意文件写入漏洞”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-2022-44687
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44686
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44689
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44688
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44704
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44703
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44707
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44706

4、 Siemens 产品安全漏洞

SINEMA Remote Connect 是一个远程网络管理平台，可轻松管理总部、服务技术人员和已安装机器或工厂之间的隧道连接 (VPN)。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。Xpedition Enterprise 是一款 PCB 设计流程，提供从系统设计定义到制造执行的集成。SICAM GridEdge 只需单击几下即可使您现有的 IEC61850 设备具有物联网功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞创建具有管理权限的新用户，更改用户的数据，注入任意代码并提升权限等。

CNVD 收录的相关漏洞包括：Siemens SINEMA Remote Connect Server 用户管理错误漏洞、Siemens SINEMA Remote Connect Server 数据真实性验证错误漏洞、Siemens SINEMA Remote Connect Server 身份验证错误漏洞、Siemens Mendix SAML Module 跨站脚本漏洞、Siemens Xpedition Designer 本地权限提升漏洞、Siemens SICAM GridEdge 身份验证错误漏洞（CNVD-2022-45216）、Siemens SICAM GridEdge 资源泄漏漏洞、Siemens SICAM GridEdge 身份验证错误漏洞。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-2022-45221
https://www.cnvd.org.cn/flaw/show/CNVD-2022-45227
https://www.cnvd.org.cn/flaw/show/CNVD-2022-45229
https://www.cnvd.org.cn/flaw/show/CNVD-2022-45212
https://www.cnvd.org.cn/flaw/show/CNVD-2022-45209
https://www.cnvd.org.cn/flaw/show/CNVD-2022-45216

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45215

https://www.cnvd.org.cn/flaw/show/CNVD-2022-45217

5、D-Link DIR-816 A2 命令注入漏洞（CNVD-2022-45933）

D-Link DIR-816 A2 是中国台湾友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-816 A2 被披露存在命令注入漏洞。该漏洞源于/goform/setSysAdm 中的 admuser 和 admpass 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通过精心设计的负载将权限提升到 root。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-2022-45933

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-2022-44736	Badminton Center Management System SQL 注入漏洞（CNVD-2022-44736）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/yasinyildiz26/Badminton-Center-Management-System
CNVD-2022-44969	WordPress PS PHPCaptcha WP 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/ps-phpcaptcha/#developers
CNVD-2022-45128	Powertek PDU 缓冲区溢出漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://www.powertekpdus.com
CNVD-2022-45213	Siemens Mendix SAML Module XML 外部实体引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-740594.html
CNVD-2022-46164	Tenda HG6 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://www.tendacn.com/product/HG6.html
CNVD-2022-46163	H3C Magic R100 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://www.h3c.com/cn/d_201801/1060028_30005_0.htm
CNVD-2022-46162	WordPress plugin RSVPMaker SQL 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://www.wordfence.com/vulnerability-advisories/#CVE-2022-1750

CNVD-2022-46168	WeCube 目录遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/WeBankPartners/wecube-platform/releases/tag/v3.2.2
CNVD-2022-45129	Powertek PDU 认证绕过漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://www.powertekpdus.com
CNVD-2022-45233	Siemens Spectrum Power Systems 默认密码泄漏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/html/ssa-388239.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞读取系统上的敏感信息，在目标系统上执行任意代码。此外，Google、Cisco、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞访问底层操作系统上的敏感文件，创建具有管理权限的新用户，更改用户的数据，执行任意脚本代码，导致权限提升，造成拒绝服务条件（DoS）等。另外，D-Link DIR-816 A2 被披露存在命令注入漏洞。攻击者可利用该漏洞通过精心设计的负载将权限提升到 root。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、CSCMS Music Portal System SQL 注入漏洞

验证描述

CSCMS Music Portal System 是中国崇胜网络科技（CSCMS）公司的一个多元化内容管理系统。

CSCMS Music Portal System 存在 SQL 注入漏洞，该漏洞源于/admin.php/vod/admin/topic/del 中的 id 参数缺少对外部输入 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://github.com/chshcms/cscms/issues/36

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-45395

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. Zimbra 曝安全漏洞，黑客无需密码即可登录

Zimbra 某些版本被披露存在安全漏洞，通过利用该漏洞，黑客可以在没有身份验证或用户交互的情况下窃取登录信息。

参考链接：https://www.bleepingcomputer.com/news/security/zimbra-bug-allows-stealing-email-logins-with-no-user-interaction/

2. 思科电子邮件存在安全漏洞，攻击者可利用漏洞登录其 Web 管理界面

思科（CISCO）于本周通知其用户修补一个严重漏洞，该漏洞可能允许攻击者绕过身份验证并登录到思科电子邮件网关设备的 Web 管理界面。

参考链接：https://www.bleepingcomputer.com/news/security/cisco-secure-email-bug-can-let-attackers-bypass-authentication/

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