国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 04 月 12 日-2021 年 04 月 18 日　　2021 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 569 个，其中高危漏洞 147 个、中危漏洞 352 个、低危漏洞 70 个。漏洞平均分值为 5.66。本周收录的漏洞中，涉及 0day 漏洞 208 个（占 37%），其中互联网上出现“Remote Clinic 跨站脚本漏洞、WCMS 目录遍历漏洞（CNVD-2021-28257）”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 3828 个，与上周（3147 个）环比增加 22%。

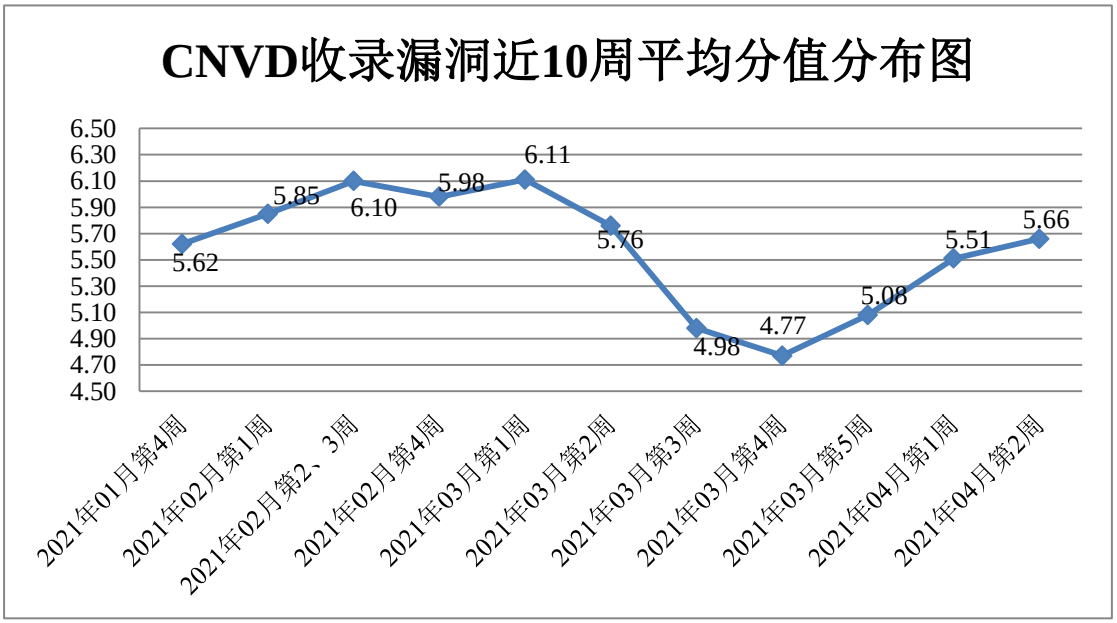

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 起，向基础电信企业通报漏洞事件 8 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 388 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 77 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 38 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、珠海金山办公软件有限公司、中控泰科（北京）科技发展有限公司、正方软件股份有限公司、浙江齐治科技股份有限公司、长沙米拓信息技术有限公司、漳州市芗城帝兴软件开发有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、微软（中国）有限公司、天津神舟通用数据技术有限公司、苏州科达科技股份有限公司、深圳市蓝凌软件股份有限公司、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、深圳市惠尔顿信息技术有限公司、深圳市共济科技股份有限公司、深圳市宝瑞明科技有限公司、深圳齐心好视通云计算有限公司、上海鸣志电器股份有限公司、上海梦之路数字科技有限公司、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、上海昂毅多媒体科技有限公司、山石网科通信技术股份有限公司、山东潍微科技股份有限公司、厦门网中网软件有限公司、厦门今点通科技发展有限公司、三星（中国）投资有限公司、锐捷网络股份有限公司、普联技术有限公司、浪潮集团有限公司、江苏三步科技股份有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南考试在线网络科技有限公司、湖南翱云网络科技有限公司、衡水金航计算机科技有限公司、河北鑫考教育科技股份有限公司、杭州荷花软件有限公司、汉王科技股份有限公司、桂林崇胜网络科技有限公司、广州网易计算机系统有限公司、广州万户网络技术有限公司、广州市奥威亚电子科技有限公司、广州酷狗计算机科技有限公司、广东微云科技股份有限公司、富士施乐（中国）有限公司、得到（天津）文化传播有限公司、大连华天软件有限公司、毕埃慕（上海）建筑数据技术股份有限公司、北京用友政务软件股份有限公司、北京网御星云信息技术有限公司、北京猎鹰安全科技有限公司、北京杰控科技有限公司、北京华夏大地远程教育网络服务有限公司、北京当当科文电子商务有限公司、北京爱奇艺科技有限公司、宝供物流企业集团有限公司、安徽旭帆信息科技有限公司、安徽省科迅教育装备有限公司、安徽科迅教育装备集团有限公司、深圳好生意网络工作室、睿谷信息管理系统、帝云 CMS、快排 CMS、YYCMS、SEMCMS、Ke361、Jpress、hybbs 和 Adobe。

本周，CNVD 发布了《Microsoft 发布 2021 年 4 月安全更新》、《关于 Google Chrome 存在远程代码执行漏洞的安全公告》、《关于 Google V8 引擎远程代码执行漏洞导致微信等软件存在关联漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6321

https://www.cnvd.org.cn/webinfo/show/6326

https://www.cnvd.org.cn/webinfo/show/6331

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、华为技术有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、天津市国瑞数码安全系统股份有限公司等单位报送公开收集的漏洞数量较多。北京信联科汇科技有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司、安徽长泰信息安全服务有限公司、北京顶象技术有限公司、西门子（中国）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、杭州海康威视数字技术股份有限公司、北京安帝科技有限公司、杭州迪普科技股份有限公司、安徽岚胜信息技术服务有限公司、木链科技、星云博创科技有限公司、武汉明嘉信信息安全检测评估有限公司、福建省海峡信息技术有限公司、物鼎安全科技（武汉）有限公司、新疆天山智汇信息科技有限公司、山石网科通信技术股份有限公司、日照天鏊网络科技有限公司、泽鹿安全、上海犀点意象网络科技有限公司、上海市信息安全测评认证中心、亚信科技（成都）有限公司、深圳开源互联网安全技术有限公司、浙江御安信息技术有限公司、广州安亿信软件科技有限公司、深圳市魔方安全科技有限公司、小安（北京）科技有限公司及其他个人白帽子向 CNVD 提交了 3828 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 2381 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）	1003	1003
上海交大	881	881
奇安信网神（补天平台）	497	497
哈尔滨安天科技集团股份有限公司	230	0
华为技术有限公司	191	0
深信服科技股份有限公司	177	5
北京天融信网络安全技术有限公司	172	6
天津市国瑞数码安全系统股份有限公司	115	115
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	51	0

北京神州绿盟科技有限公司	49	4
北京启明星辰信息安全技术有限公司	40	0
中国电信股份有限公司网络安全产品运营中心	30	10
中国电信集团系统集成有限责任公司	19	19
北京长亭科技有限公司	8	8
远江盛邦（北京）网络安全科技股份有限公司	4	4
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
北京智游网安科技有限公司	1	1
北京信联科汇科技有限公司	238	238
山东新潮信息技术有限公司	79	79
河南灵创电子科技有限公司	26	26
安徽长泰信息安全服务有限公司	25	25
北京顶象技术有限公司	25	25
西门子（中国）有限公司	20	0
北京天地和兴科技有限公司	10	10
河南信安世纪科技有限公司	10	10
杭州海康威视数字技术股份有限公司	8	8
北京安帝科技有限公司	7	7
杭州迪普科技股份有限公司	5	0

安徽岚胜信息技术服务有限公司	5	5
木链科技	4	4
星云博创科技有限公司	4	4
武汉明嘉信信息安全检测评估有限公司	4	4
福建省海峡信息技术有限公司	3	3
物鼎安全科技（武汉）有限公司	3	3
新疆天山智汇信息科技有限公司	2	2
山石网科通信技术股份有限公司	2	2
日照天鋆网络科技有限公司	2	2
泽鹿安全	2	2
上海犀点意象网络科技有限公司	1	1
上海市信息安全测评认证中心	1	1
亚信科技（成都）有限公司	1	1
深圳开源互联网安全技术有限公司	1	1
浙江御安信息技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
小安（北京）科技有限公司	1	1
CNCERT 青海分中心	8	8
个人	799	799
报送总计	4885	3828

本周漏洞按类型和厂商统计

本周，CNVD 收录了 569 个漏洞。应用程序 259 个，WEB 应用 160 个，操作系统 72 个，网络设备（交换机、路由器等网络端设备）45 个，安全产品 27 个，智能设备（物

联网终端设备）5 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	259
WEB 应用	160
操作系统	72
网络设备（交换机、路由器等网络端设备）	45
安全产品	27
智能设备（物联网终端设备）漏洞	5
数据库	1

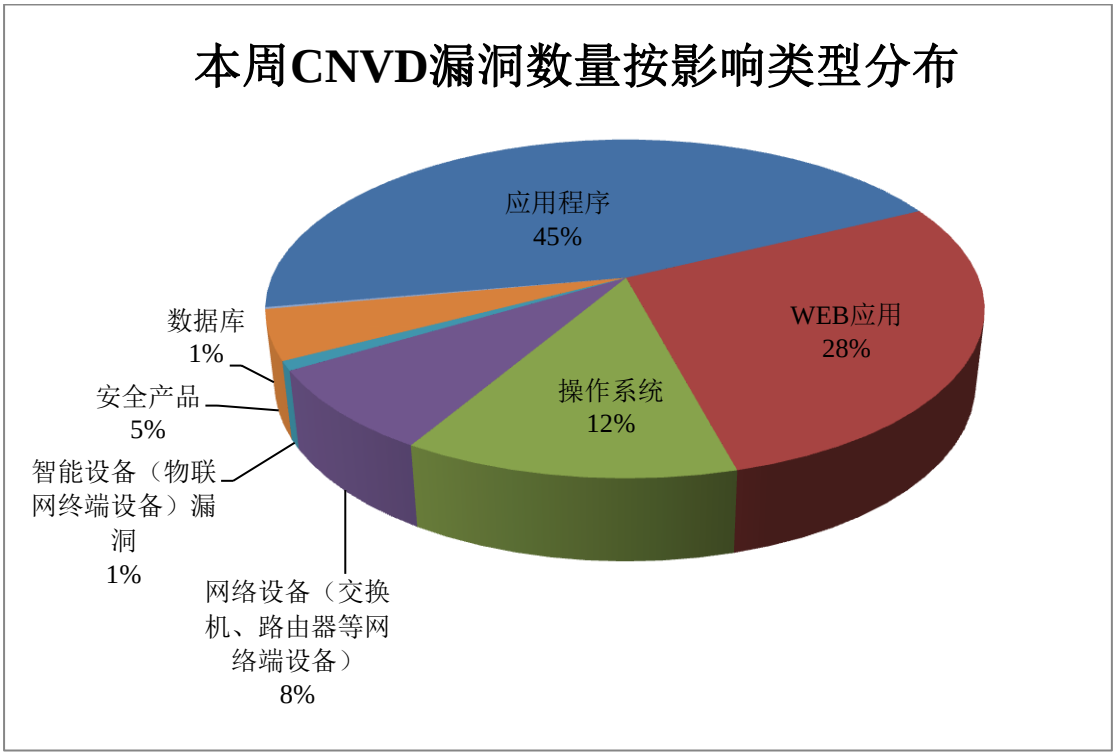

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、华夏 ERP 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	38	7%
2	Microsoft	34	6%
3	华夏 ERP	25	4%
4	SEMCMS	22	4%
5	Siemens	20	4%
6	NVIDIA	20	4%
7	Trend Micro	19	3%
8	XStream	12	2%

9	SonicWall	12	2%
10	其他	367	64%

本周行业漏洞收录情况

本周，CNVD 收录了 29 个电信行业漏洞，35 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，“Brocade Fabric OS 缓冲区溢出漏洞、Google Android System 权限提升漏洞（CNVD-2021-29045）、Siemens Nucleus 产品越界写入漏洞、Advantech Spectre RT ERT351 暴力破解漏洞、Cisco Catalyst 9800 Series Wireless Controllers IOS XE Software 资源管理错误漏洞”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/

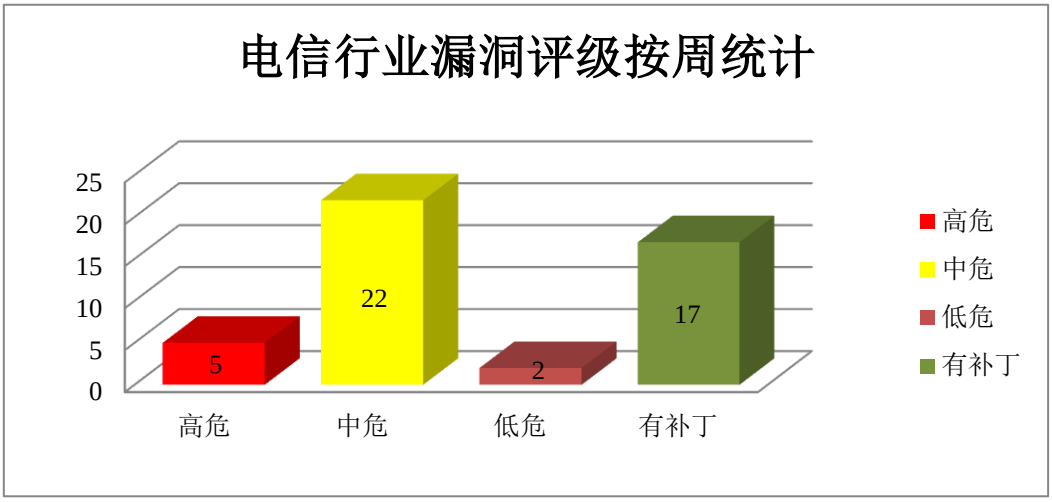

图 3 电信行业漏洞统计

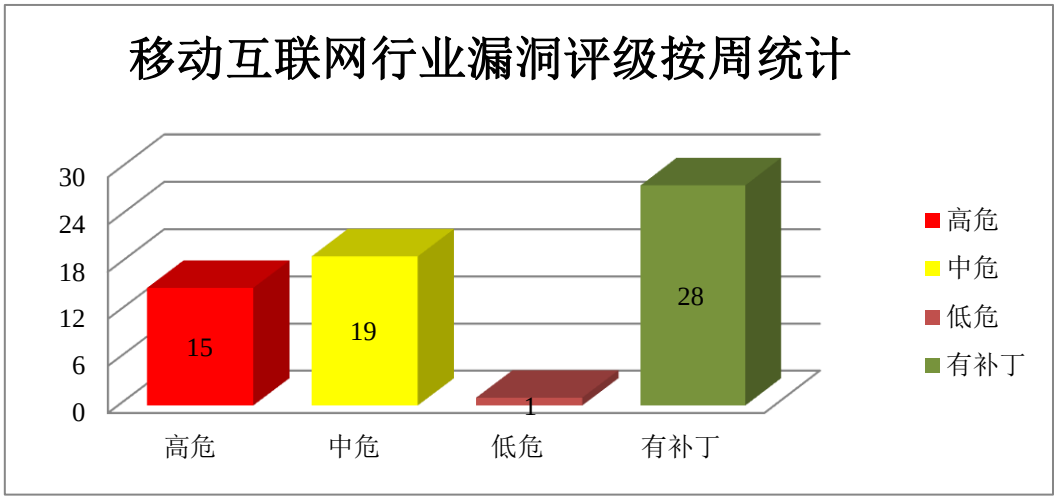

图 4 移动互联网行业漏洞统计

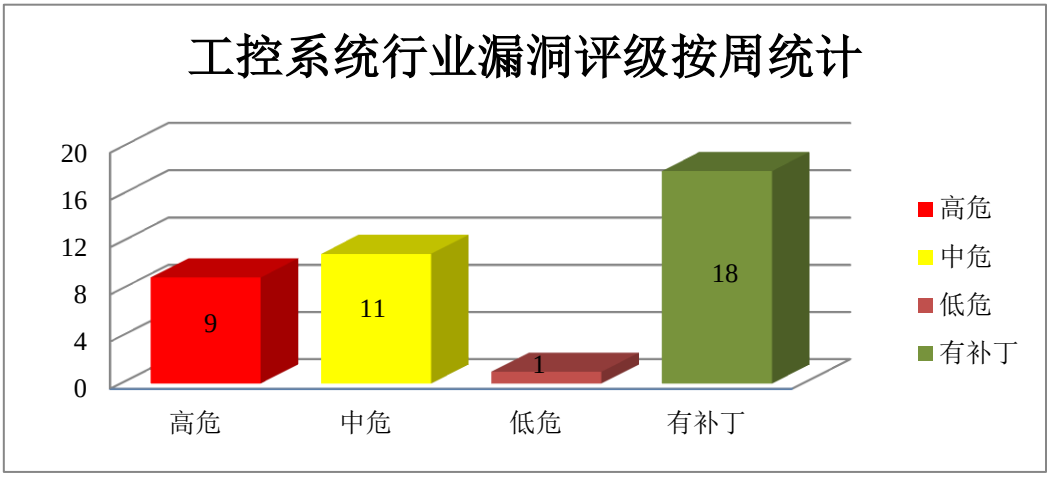

图 5 工控系统行业漏洞统计

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 Mendix 是德国西门子（Siemens）公司的一套低代码应用程序开发平台。Siemens Solid Edge 是一款三维 CAD 软件。Nucleus NET 模块包含了一系列符合标准的网络和通信协议、驱动程序和实用程序，以在任何嵌入式设备中提供全功能的网络支持。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管理权限，执行代码，导致无限循环和拒绝服务等。

CNVD 收录的相关漏洞包括：Siemens Solid Edge PAR 文件越界写入漏洞、Siemens Solid Edge PAR 文件堆栈缓冲区溢出漏洞、Siemens Solid Edge PAR 文件不可信指针解引用漏洞、Siemens Nucleus 产品 IPv6 堆栈拒绝服务漏洞、Siemens Nucleus 产品 IPv6 堆栈拒绝服务漏洞（CNVD-2021-28696）、Siemens Nucleus 产品越界写入漏洞（CNVD-2021-28701、CNVD-2021-28702）、Siemens Mendix 权限提升漏洞。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-2021-28694

https://www.cnvd.org.cn/flaw/show/CNVD-2021-28693

https://www.cnvd.org.cn/flaw/show/CNVD-2021-28697

https://www.cnvd.org.cn/flaw/show/CNVD-2021-28696

https://www.cnvd.org.cn/flaw/show/CNVD-2021-28695

https://www.cnvd.org.cn/flaw/show/CNVD-2021-28701

https://www.cnvd.org.cn/flaw/show/CNVD-2021-28702

https://www.cnvd.org.cn/flaw/show/CNVD-2021-28717

2、Microsoft 产品安全漏洞

Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Windows Installer 是其中的一个基于 Windows 系统的工具组件，主要用于管理和配置软件服务。Microsoft Exchange Server 是一套电子邮件服务程序。Microsoft Visual Studio 是一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，使用 XML 内容覆盖任意文件，执行任意代码，导致程序崩溃等。

CNVD 收录的相关漏洞包括：Microsoft Windows Modules Installer Service 权限提升漏洞、Microsoft Windows Installer 权限提升漏洞（CNVD-2021-27710）、Microsoft Visual Studio 权限提升漏洞、Microsoft Exchange Server 拒绝服务漏洞、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2021-29060、CNVD-2021-29061、CNVD-2021-29062、CNVD-2021-29063）。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-2021-27704
https://www.cnvd.org.cn/flaw/show/CNVD-2021-27710
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28804
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28825
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29060
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29061
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29062
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29063

3、Eclipse 产品安全漏洞

Eclipse Jetty 是 Eclipse 基金会的一个开源的、基于 Java 的 Web 服务器和 Java Servlet 容器。Eclipse Mosquitto 是实现 3.1 和 3.1.1 版 MQTT 协议的开源（EPL/EDL 许可）消息代理。Eclipse Platform 是 Eclipse 开源的定义了一组框架和公共服务，共同构成了支持将 Eclipse 作为组件模型，富客户端平台（RCP）和全面的工具集成平台的使用所需的基础结构。用于管理资源的项目模型，用于增量编译器和构建器的自动资源增量管理，与语言无关的调试基础结构以及用于分布式多用户版本化资源管理的基础结构。Eclipse Vertx-web 是一个用于构建 Web 应用的框架。Eclipse Mosquitto 是一套开源的消息代理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，导致空指针解引用，CSRF 攻击和跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Eclipse Mosquitto 空指针解引用漏洞、Eclipse Mosq

uitto 资源管理错误漏洞、Eclipse Jetty 权限绕过漏洞、Eclipse Jetty 信息泄露漏洞（CNVD-2021-28269）、Eclipse Jetty HTTP 请求走私漏洞、Eclipse Jetty 跨站脚本漏洞（CNVD-2021-28275）、Eclipse Platform 未授权访问漏洞、Eclipse Vertx-web 跨站请求伪造漏洞。其中，“Eclipse Jetty 信息泄露漏洞（CNVD-2021-28269）、Eclipse Jetty HTTP 请求走私漏洞”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-2021-27363
https://www.cnvd.org.cn/flaw/show/CNVD-2021-27374
https://www.cnvd.org.cn/flaw/show/CNVD-2021-27383
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28266
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28269
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28268
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28276
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28275

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。Android 是一套以 Linux 为基础的开源操作系统。Airbrush 是其中的一个照片编辑器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致堆破坏等。

CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用漏洞（CNVD-2021-27268、CNVD-2021-27269）、Google Chrome 堆缓冲区溢出漏洞（CNVD-2021-28284）、Google Chrome 释放后重用漏洞（CNVD-2021-28286、CNVD-2021-28287）、Google Android System 远程代码执行漏洞（CNVD-2021-29047）、Google V8 引擎远程代码执行漏洞、Android Airbrush 权限提升漏洞。其中，除 “Google Chrome 堆缓冲区溢出漏洞（CNVD-2021-28284）、Google Chrome 释放后重用漏洞（CNVD-2021-28286、CNVD-2021-28287）”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-2021-27268
https://www.cnvd.org.cn/flaw/show/CNVD-2021-27269
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28007
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28284
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28286
https://www.cnvd.org.cn/flaw/show/CNVD-2021-28287
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29047
https://www.cnvd.org.cn/flaw/show/CNVD-2021-29059

5、Zoom 远程代码执行漏洞

Zoom 是现代企业视频通讯领域的领导者，可以为跨移动设备、台式机和会议室系统的视频/音频会议、协作、聊天和网络研讨会提供平台。本周，Zoom 被披露存在远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造的会话请求，无需用户交互，获得目标服务器的权限，实现远程代码执行攻击。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-2021-27997

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-2021-27799	UX360CA BIOS through 303 on ASUS 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.asus.com/support/FAQ/1045541/
CNVD-2021-28000	Cisco Catalyst 9800 Series Wireless Controllers IOS XE Software 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ewlc-dos-TkuPVmZN
CNVD-2021-28013	NETGEAR ReadyNAS Surveillance 跨站请求伪造漏洞	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/000038435/Security-Advisory-for-ReadyNAS-Surveillance-CSRF-Remote-Code-Execution-PSV-2017-0578
CNVD-2021-28299	Mozilla Thunderbird 拒绝服务漏洞（CNVD-2021-28299）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2021-13/
CNVD-2021-28324	多款Trend Micro产品缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://success.trendmicro.com/solution/000284206 https://success.trendmicro.com/solution/000284205 https://success.trendmicro.com/solution/000284202
CNVD-2021-28764	SonicWALL SonicOS 缓冲区溢出漏洞（CNVD-2021-28764）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://psirt.global.sonicwall.com/vuln-

			detail/SNWLID-2020-0010
CNVD-2021-28796	Juniper Networks NFX Series Junos OS 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://kb.juniper.net/InfoCenter/index?page=content&id=JSA10977&actp=METADATA
CNVD-2021-29082	FreeBSD 缓冲区溢出漏洞（CNVD-2021-29082）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.cybersecurity-help.cz/vdb/SB2020090303
CNVD-2021-29098	SAP NetWeaver Application Server for Java 信息泄露漏洞	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=573801649
CNVD-2021-29109	Adobe Photoshop 缓冲区溢出漏洞（CNVD-2021-29109）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/photoshop/apsb21-28.html

小结：本周，Siemens 产品被披露存在多个漏洞，攻击者可利用漏洞获取管理权限，执行代码，导致无限循环和拒绝服务等。此外，Microsoft、Eclipse、Google 等多款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，使用 XML 内容覆盖任意文件，执行任意代码，导致空指针解引用，CSRF 攻击和跨站脚本攻击，程序崩溃和堆破坏等。另外，Zoom 被披露存在远程代码执行漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造的会话请求，无需用户交互，获得目标服务器的权限，实现远程代码执行攻击。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、Remote Clinic 跨站脚本漏洞

验证描述

Remote Clinic 是一款开源诊所管理系统，可让您通过 Web 远程管理您的诊所。

Remote Clinic v2.0 版本存在跨站脚本漏洞。攻击者可通过 staff/register.php 的 First Name 或 Last Name 字段利用该漏洞注入任意脚本或 html。

验证信息

POC 链接：https://github.com/remoteclinic/RemoteClinic/issues/13

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-28265

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. 微信被曝高危 0day 漏洞，建议立即更新

4 月 16 日，微信 PC 版客户端被曝存在一个高危等级的在野 0day 漏洞。目前，微信已修复漏洞并发布了更新版本，强烈建议大家立即将微信更新到 3.2.1.141 以上版本修复漏洞。

参考链接：https://www.freebuf.com/news/269896.html

2. SAP 修复了 Business Client，Commerce 和 NetWeaver 中的严重漏洞

SAP 本月的安全更新解决了多个关键漏洞。其中最严重的评分最高，会影响公司的 Business Client 产品。该公司的另外两个产品收到了针对严重缺陷漏洞的补丁程序，这些漏洞使未经授权的用户可以访问配置对象并允许远程执行代码。

参考链接：https://www.bleepingcomputer.com/news/security/sap-fixes-critical-bugs-in-business-client-commerce-and-netweaver

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