国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 12 月 27 日-2022 年 01 月 02 日　　2021 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 534 个，其中高危漏洞 139 个、中危漏洞 320 个、低危漏洞 75 个。漏洞平均分值为 5.68。本周收录的漏洞中，涉及 0day 漏洞 197 个（占 37%），其中互联网上出现“Wordpress 插件 Download From Files 任意文件上传漏洞、WordPress Popular Posts 远程代码执行漏洞（CNVD-2021-102873）”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 36493 个，与上周（19707 个）环比增加 85%。

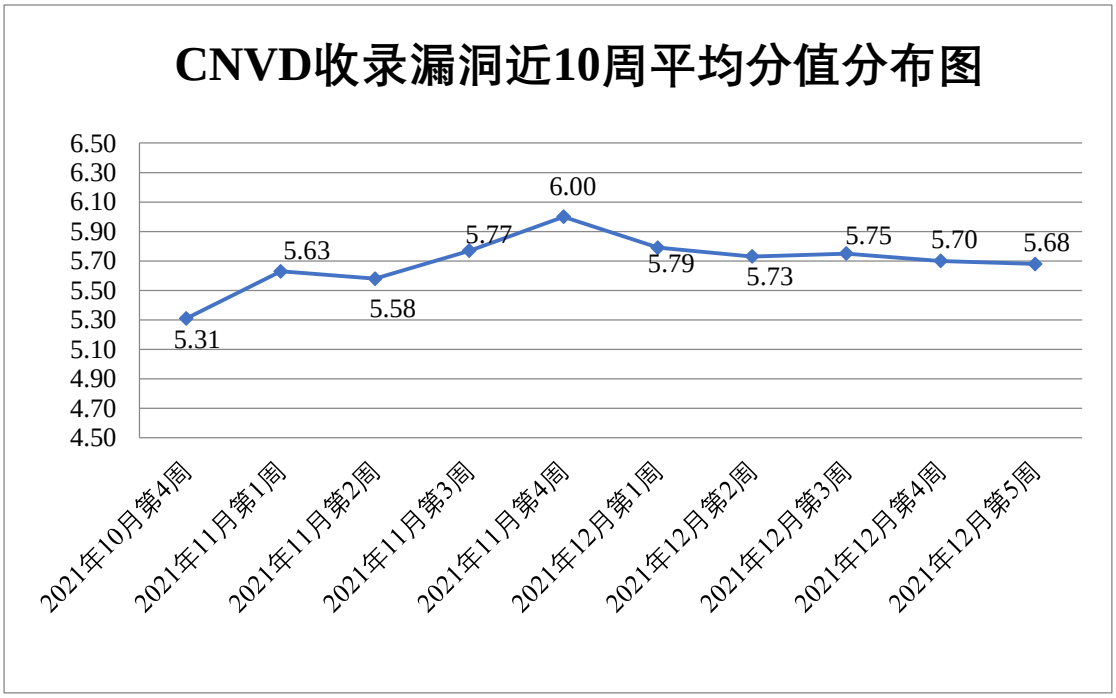

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电

信企业通报漏洞事件 20 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 525 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 61 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 74 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、淄博闪灵网络科技有限公司、重庆朗奕迪实业有限公司、中国建筑第八工程局有限公司、浙江兰德纵横网路技术股份有限公司、浙江多普勒环保科技有限公司、长沙米拓信息技术有限公司、云梦吧网络资讯工作室、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、新天科技股份有限公司、新开普电子股份有限公司、襄阳智博珞格网络科技有限公司、西门子（中国）有限公司、武汉赢卓科技有限公司、武汉神州数码云科网络技术有限公司、微软（中国）有限公司、天津神州浩天科技有限公司、台湾永宏电机股份有限公司、苏州市亿韵商务信息有限公司、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、深圳英迈思信息技术有限公司、深圳市易智达信息技术有限公司、深圳市网域科技技术有限公司、深圳市万普拉斯科技有限公司、深圳市捷视飞通科技股份有限公司、深圳市博思协创网络科技有限公司、上海纵之格科技有限公司、上海易正信息技术有限公司、上海华测导航技术股份有限公司、上海孚盟软件有限公司、上海泛微网络科技股份有限公司、山西企凝信息科技有限公司、山石网科通信技术（北京）有限公司、山东智工云网络科技有限公司、山东金钟科技集团股份有限公司、厦门一指通智能科技有限公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、厦门科拓通讯技术股份有限公司、厦门海为科技有限公司、普联技术有限公司、罗克韦尔自动化（中国）有限公司、浪潮通用软件有限公司、蓝网科技股份有限公司、敬业钢铁有限公司、江苏亿友慧云软件股份有限公司、佳都科技集团股份有限公司、吉翁电子（深圳）有限公司、华平信息技术股份有限公司、湖南三唐信息科技有限公司、湖南康通电子股份有限公司、浩通国际货运代理有限公司、杭州可道云网络有限公司、杭州迪普科技股份有限公司、哈尔滨伟成科技有限公司、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、广州瑾祺信息科技有限公司、广州安网通信技术有限公司、福建银达汇智信息科技股份有限公司、福建福昕软件开发股份有限公司、北京字节跳动科技有限公司、北京中科网威信息技术有限公司、北京致远互联软件股份有限公司、北京雪迪龙科技股份有限公司、北京万户互联科技有限公司、北京数科网维技术有限责任公司、北京朗新天霁软件技术有限公司、北京九思协同软件有限公司、北京互动百科网络技术有限公司、北京和信创天科技股份有限公司、北京国通创安报警网络技术有限公司、北京飞书科技有限公司、北京百容千域软件技术开发有限责任公司、北京爱奇艺科技有限公司、安徽省科大奥锐科技有限公司、北京和利时集团、信呼、谷歌公司、zzcms、XnSoft、VideoLAN、

The Apache Software Foundation、taocms、Sapido Technology Inc、Irfan Skiljan、Iceni Technology Limited、Grafana Labs、Glyph & Cog, LLC、Dnsmasq 和 BANDISOFT。

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、恒安嘉新（北京）科技股份公司、西安四叶草信息技术有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。北京山石网科信息技术有限公司、河南灵创电子科技有限公司、南京众智维信息科技有限公司、广东蓝爵网络安全技术股份有限公司、南京树安信息技术有限公司、北京信联科汇科技有限公司、山东新潮信息技术有限公司、贵州多彩宝互联网服务有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、内蒙古洞明科技有限公司、快页信息技术有限公司、山东云天安全技术有限公司、福建省海峡信息技术有限公司、京东云安全、上海上讯信息技术股份有限公司、河南信安世纪科技有限公司、山石网科通信技术股份有限公司、重庆都会信息科技有限公司、北京远禾科技有限公司、思而听网络科技有限公司、杭州美创科技有限公司、北京快手科技有限公司、京东探索研究院信息安全实验室、中安网盾（广州）信息科技有限公司、新疆海狼科技有限公司、北京惠而特科技有限公司、平安银河实验室、广西塔易信息技术有限公司、广州安亿信软件科技有限公司、北京升鑫网络科技有限公司、上海软件中心、杭州安节科技有限公司、天津偕行科技有限公司、内蒙古云科数据服务股份有限公司、北京安帝科技有限公司、苏州棱镜七彩信息科技有限公司、浙江浙大中控信息技术有限公司及其他个人白帽子向 CNVD 提交了 36493 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）和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 34373 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）	21006	21006
奇安信网神（补天平台）	13367	13367
北京天融信网络安全技术有限公司	303	54
哈尔滨安天科技集团股份有限公司	233	0
恒安嘉新（北京）科技股份公司	128	0
西安四叶草信息技术	126	126

有限公司		
深信服科技股份有限公司	117	0
北京神州绿盟科技有限公司	113	8
杭州安恒信息技术股份有限公司	80	80
新华三技术有限公司	66	0
天津市国瑞数码安全系统股份有限公司	58	0
北京启明星辰信息安全技术有限公司	51	3
远江盛邦（北京）网络安全科技股份有限公司	45	45
中国电信集团系统集成有限责任公司	30	0
北京数字观星科技有限公司	23	0
北京知道创宇信息技术股份有限公司	6	1
南京联成科技发展股份有限公司	5	5
北京智游网安科技有限公司	1	1
北京华顺信安科技有限公司	219	0
北京山石网科信息技术有限公司	140	140
河南灵创电子科技有限公司	90	90
南京众智维信息科技有限公司	86	86
广东蓝爵网络安全技术股份有限公司	61	61

南京树安信息技术有限公司	55	55
北京信联科汇科技有限公司	36	36
山东新潮信息技术有限公司	32	32
贵州多彩宝互联网服务有限公司	12	12
杭州迪普科技股份有限公司	29	0
北京云科安信科技有限公司（Seraph 安全实验室）	26	26
中国电信股份有限公司网络安全产品运营中心	20	0
内蒙古洞明科技有限公司	18	18
快页信息技术有限公司	15	15
山东云天安全技术有限公司	11	11
福建省海峡信息技术有限公司	10	10
京东云安全	10	10
上海上讯信息技术股份有限公司	8	8
河南信安世纪科技有限公司	8	8
山石网科通信技术股份有限公司	7	7
重庆都会信息科技有限公司	7	7
北京远禾科技有限公司	6	6

思而听网络科技有限公司	4	4
杭州美创科技有限公司	4	4
北京快手科技有限公司	3	3
京东探索研究院信息安全实验室	2	2
中安网盾（广州）信息科技有限公司	2	2
新疆海狼科技有限公司	2	2
亚信科技（成都）有限公司	1	0
北京惠而特科技有限公司	1	1
平安银河实验室	1	1
广西塔易信息技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京升鑫网络科技有限公司	1	1
上海软件中心	1	1
杭州安节科技有限公司	1	1
天津偕行科技有限公司	1	1
内蒙古云科数据服务股份有限公司	1	1
西门子（中国）有限公司	1	0
北京安帝科技有限公司	1	1
苏州棱镜七彩信息科	1	1

技有限公司		
浙江浙大中控信息技术有限公司	1	1
CNCERT 四川分中心	1	1
个人	1134	1129
报送总计	37830	36493

本周漏洞按类型和厂商统计

本周，CNVD 收录了 534 个漏洞。WEB 应用 245 个，应用程序 156 个，操作系统 71 个，网络设备（交换机、路由器等网络端设备）28 个，智能设备（物联网终端设备）24 个，安全产品 9 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	245
应用程序	156
操作系统	71
网络设备（交换机、路由器等网络端设备）	28
智能设备（物联网终端设备）	24
安全产品	9
数据库	1

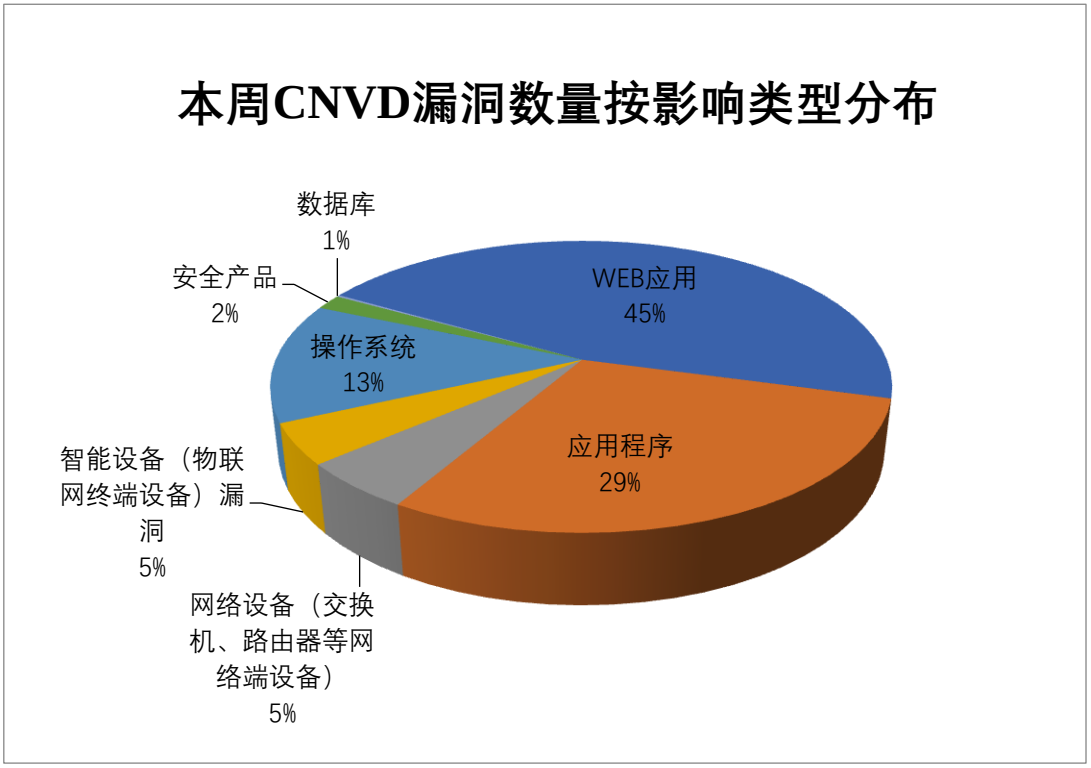

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Huawei、Google 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	WordPress	68	13%
2	Huawei	27	5%
3	Google	21	4%
4	Cisco	17	3%
5	Oracle	12	2%
6	Adobe	10	2%
7	Nextcloud	9	2%
8	Apache	11	2%
9	上海泛微网络科技股份有限公司	9	2%
10	其他	350	65%

本周行业漏洞收录情况

本周，CNVD 收录了 21 个电信行业漏洞，44 个移动互联网行业漏洞，17 个工控行业漏洞（如下图所示）。其中，“Elecom Edwrc 操作系统操作系统命令注入漏洞、Google Android 访问控制错误漏洞（CNVD-2021-103502）、Huawei Emui 和 Magic UI 数据处理错误漏洞、AVEVA System Platform 路径遍历漏洞”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/

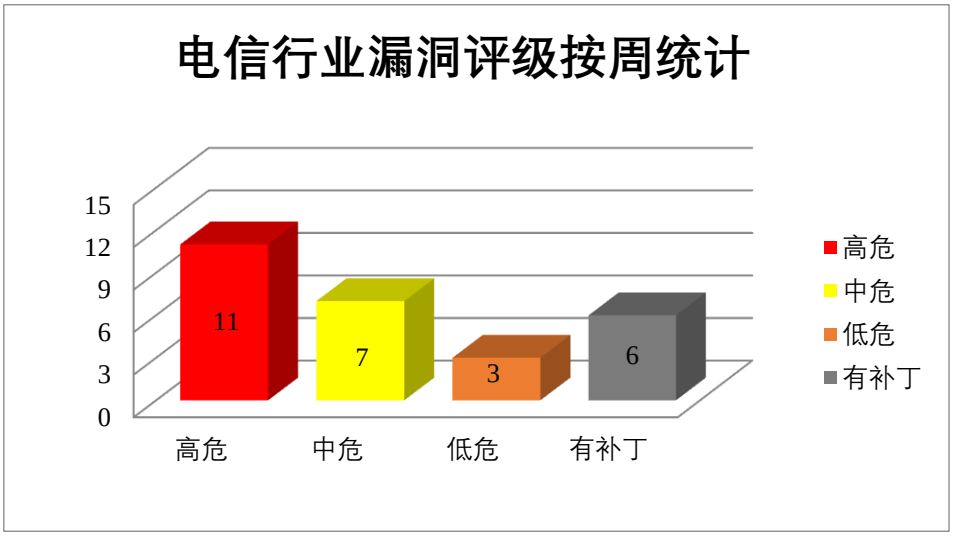

图 3 电信行业漏洞统计

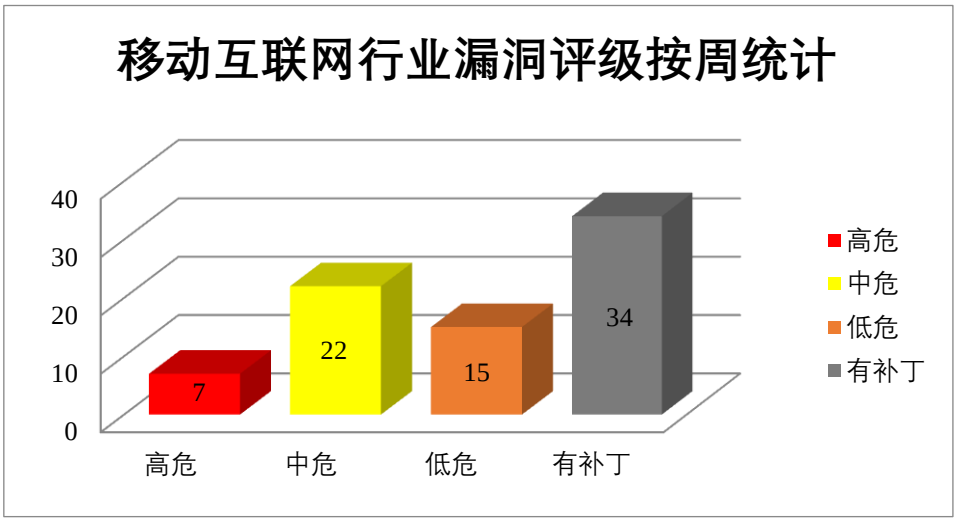

图 4 移动互联网行业漏洞统计

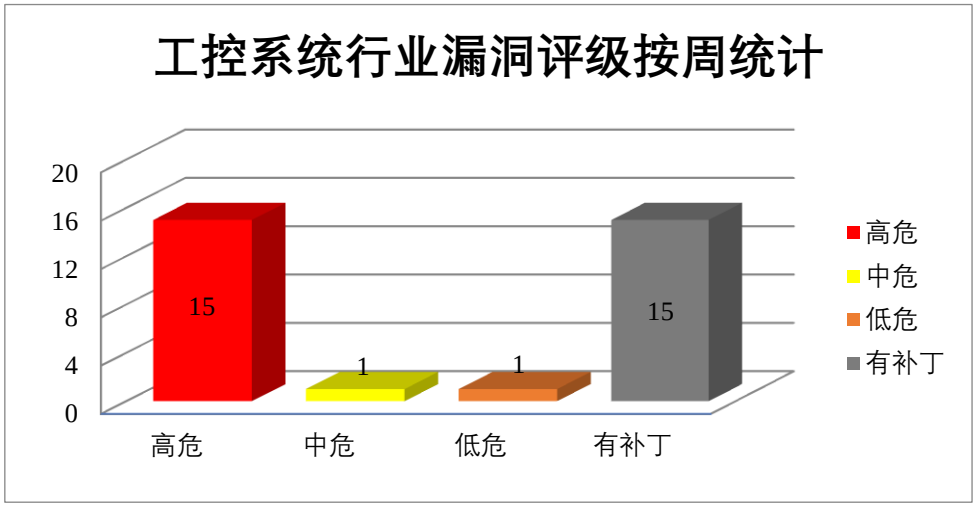

图 5 工控系统行业漏洞统计

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

Magento 是 Adobe 公司旗下一款用 PHP 编写的开源电子商务平台。Adobe Framemaker 是美国奥多比（Adobe）公司的一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。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受影响组件敏感信息，绕过安全特性，提升权限，执行任意代码，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：Adobe Magento 输入验证错误漏洞（CNVD-2021-102806、CNVD-2021-102805、CNVD-2021-102809、CNVD-2021-102808、CNVD-2021-10

2807）、Adobe Framemaker 缓冲区溢出漏洞（CNVD-2021-102813、CNVD-2021-10281 2）、Adobe Acrobat Reader 路径遍历漏洞。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-2021-102806

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102805

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102809

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102808

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102807

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102813

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102812

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102814

2、 Cisco 产品安全漏洞

Cisco IOS XR Software 是美国思科（Cisco）公司的一套为其网络设备开发的操作系统。Cisco Small Business RV Series Routers 是美国思科（Cisco）公司的一款 RV 系列路由器。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。Cisco Anyconnect Secure Mobility Client 是美国思科（Cisco）公司的一款用于安全连接的 VPN 客户端软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞向服务器发送非预期的请求，在受影响的设备上升级特权，执行任意命令等。

CNVD 收录的相关漏洞包括：Cisco IOS XR Software 任意文件读写漏洞、Cisco I OS XR Software 命令注入漏洞（CNVD-2021-102364）、Cisco IOS XR Software 权限提升漏洞（CNVD-2021-102362、CNVD-2021-102367）、Cisco IOS XR Software 拒绝服务漏洞（CNVD-2021-102366）、Cisco Small Business RV Series Routers 命令注入漏洞、Cisco Unified Communications Manager 跨站请求伪造漏洞（CNVD-2021-103095）、Cisco AnyConnect Secure Mobility Client 权限提升漏洞（CNVD-2021-103367）。其中，“Cisco IOS XR Software 任意文件读写漏洞、Cisco IOS XR Software 权限提升漏洞（CNVD-2021-102362）、Cisco Small Business RV Series Routers 命令注入漏洞、Cis co AnyConnect Secure Mobility Client 权限提升漏洞（CNVD-2021-103367）”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-2021-102365

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102364

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102362

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102367

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102366

https://www.cnvd.org.cn/flaw/show/CNVD-2021-103092

https://www.cnvd.org.cn/flaw/show/CNVD-2021-103095

https://www.cnvd.org.cn/flaw/show/CNVD-2021-103367

3、Huawei 产品安全漏洞

Huawei Emui 是一款基于 Android 开发的移动端操作系统。Magic Ui 是一款基于 Android 开发的移动端操作系统。Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。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，删除任意文件，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei Emui 和 Magic UI 数据处理错误漏洞、Huawei HarmonyOS 数组越界漏洞、Huawei HarmonyOS 越界读取漏洞（CNVD-2021-102855、CNVD-2021-103539）、Huawei HarmonyOS 堆溢出漏洞、Huawei HarmonyOS 路径遍历漏洞（CNVD-2021-103534、CNVD-2021-103541）、Huawei HarmonyOS 整数溢出漏洞（CNVD-2021-103536）。其中，除“Huawei HarmonyOS 路径遍历漏洞（CNVD-2021-103534、CNVD-2021-103541）、Huawei HarmonyOS 越界读取漏洞（CNVD-2021-103539）”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-2021-102854

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102856

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102855

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102859

https://www.cnvd.org.cn/flaw/show/CNVD-2021-103534

https://www.cnvd.org.cn/flaw/show/CNVD-2021-103536

https://www.cnvd.org.cn/flaw/show/CNVD-2021-103541

https://www.cnvd.org.cn/flaw/show/CNVD-2021-103539

4、Oracle 产品安全漏洞

Oracle Solaris 是一款类 Unix 操作系统。Oracle Transportation Management (OTM) 为公司提供了一个单一平台来管理整个供应链中的所有运输活动。Java SE 是 Java 平台标准版的简称，用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle HTTP Server 是 Oracle Fusion Middleware 的 Web 服务器组件。Oracle Hyperion Financial Reporting 是一款财务报表生成软件。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，进行未经授权的更新、插入或删除访问等。

CNVD 收录的相关漏洞包括：Oracle Solaris 拒绝服务漏洞（CNVD-2021-102406、CNVD-2021-102407）、Oracle Transportation Management 未授权访问漏洞（CNVD-2021-102408、CNVD-2021-102409）、Oracle Java SE 未授权访问漏洞、Oracle HTTP Se

rver 未授权访问漏洞（CNVD-2021-102412、CNVD-2021-102413）、Oracle Hyperion Financial Reporting 未授权访问漏洞。其中，“Oracle HTTP Server 未授权访问漏洞”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-2021-102406
https://www.cnvd.org.cn/flaw/show/CNVD-2021-102408
https://www.cnvd.org.cn/flaw/show/CNVD-2021-102407
https://www.cnvd.org.cn/flaw/show/CNVD-2021-102410
https://www.cnvd.org.cn/flaw/show/CNVD-2021-102409
https://www.cnvd.org.cn/flaw/show/CNVD-2021-102412
https://www.cnvd.org.cn/flaw/show/CNVD-2021-102411
https://www.cnvd.org.cn/flaw/show/CNVD-2021-102413

5、ZZCMS SQL 注入漏洞（CNVD-2021-103084）

ZZCMS 是中国 ZZCMS 团队的一套内容管理系统（CMS）。本周，ZZCMS 被披露存在 SQL 注入漏洞。该漏洞源于在 dl/dl_download.php 中注册普通用户时缺少对外部输入 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。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-2021-103084

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-2021-102375	Arista Networks MOS 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.arista.com/en/support/advisories-notices/security-advisories/12912-security-advisory-64
CNVD-2021-102386	Apache HTTP Server 缓冲区溢出漏洞（CNVD-2021-102386）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://httpd.apache.org/download.cgi#apache24
CNVD-2021-102789	WordPress WooCommerce Multivendor Marketplace 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://wpscan.com/vulnerability/763c08a0-4b2b-4487-b91c-be6cc2b9322e
CNVD-2021-102829	mySCADA myPRO 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.myscada.org/version-8-22-0-released-security-update/
CNVD-2021-102869	Microsoft Outlook 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，详情请关注厂商主页：https://www.microsoft.com/zh-cn/microsoft-365/outlook/outlook-for-business
CNVD-2021-102885	OpenSIS Community Edition 本地文件包含漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://opensis.com
CNVD-2021-103365	Apostrophe 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://github.com/apostrophecms/apostrophe/commit/c211b211f9f4303a77a307cf41aac9b4ef8d2c7c
CNVD-2021-103502	Google Android 访问控制错误漏洞（CNVD-2021-103502）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/aaos/2021-12-01
CNVD-2021-103655	Juniper Networks Junos OS 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://kb.juniper.net/InfoCenter/index?page=content&id=JSA11252&actp=SUBSCRIPTION
CNVD-2021-103660	ThinkPHP SQL 注入漏洞（CNVD-2021-103660）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/top-think/framework/issues/2613

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞获取受影响组件敏感信息，绕过安全特性，提升权限，执行任意代码，导致缓冲区溢出或堆溢出等。此外，Cisco、Huawei、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞向服务器发送非预期的请求，获取敏感信息，删除任意文件，在受影响的设备上升级特权，执行任意命令，导致拒绝服务等。另外，ZZCMS 被披露存在 SQL 注入漏洞。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。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、Wordpress 插件 Download From Files 任意文件上传漏洞

验证描述

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。WordPress Download From Files 是一个文件中转及下载软件。

Wordpress 插件 Download From Files 存在任意文件上传漏洞。攻击者可利用漏洞上传 webshell，获得服务器权限。

验证信息

POC 链接：https://www.exploit-db.com/exploits/50287

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-102874

信息提供者

深信服科技股份有限公司

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. DataVault 加密软件中的缺陷影响多个存储设备

安全研究人员发现，由 ENC Security 制造并被多家供应商使用的 DataVault 加密软件存在严重安全漏洞，攻击者利用该漏洞可获取用户密码。

参考链接：https://securityaffairs.co/wordpress/126166/hacking/datavault-encryption-software-flaws.html

2. 地铁安防门被曝存在多个严重的安全漏洞

近日发现，Garrett 金属探测器的网络组件中存在许多严重的安全漏洞。这些漏洞可能允许远程攻击者绕过身份验证要求、篡改金属探测器配置，甚至在设备上执行任意代码。

参考链接：https://www.freebuf.com/news/317879.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