国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 11 月 15 日-2021 年 11 月 20 日　　2021 年第 46 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 585 个，其中高危漏洞 137 个、中危漏洞 409 个、低危漏洞 39 个。漏洞平均分值为 5.77。本周收录的漏洞中，涉及 0day 漏洞 393 个（占 67%），其中互联网上出现“AyaCMS 跨站请求伪造漏洞、Sourcecodester Complaint 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原创漏洞总数 10498 个，与上周（20493 个）环比减少 49%。

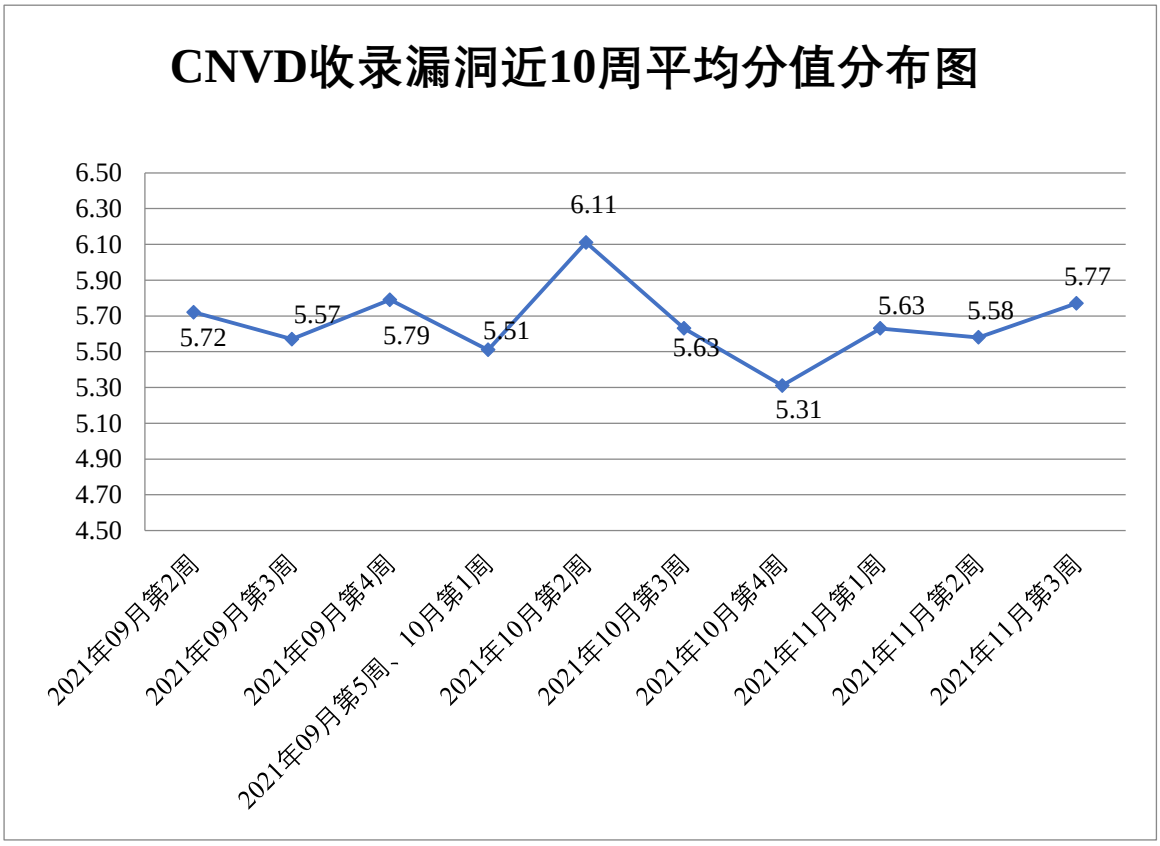

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 18 起，向基础电信企业通报漏洞事件 41 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 826 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 109 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 84 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、珠海玖时光科技有限公司、珠海金山办公软件有限公司、中国船舶重工集团国际工程有限公司、浙江中易慧能科技有限公司、浙江宇视科技有限公司、浙江蓝联科技股份有限公司、浙江大华技术股份有限公司、长沙市同迅计算机科技有限公司、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、新天科技股份有限公司、武汉盛帆电子股份有限公司、武汉达梦数据库股份有限公司、微软（中国）有限公司、松下电器（中国）有限公司、思科系统（中国）网络技术有限公司、视联动力信息技术股份有限公司、世邦通信股份有限公司、石家庄市征红网络科技有限公司、深圳维盟科技股份有限公司、深圳市宇隆移动互联网有限公司、深圳市微客互动有限公司、深圳市网心科技有限公司、深圳市华波美通信技术有限公司、深圳市皓峰通讯技术有限公司、深圳市必联电子有限公司、深圳警翼智能科技股份有限公司、深电能科技集团有限公司、上海亿速网络科技有限公司、上海星鸟网络科技有限公司、上海建文软件科技有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、山石网科通信技术股份有限公司、山东山大华天软件有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、普联技术有限公司、南京云网汇联软件技术有限公司、南京旭顶通讯科技有限公司、南京科远智慧科技集团股份有限公司、罗技（中国）科技有限公司、龙采科技集团有限责任公司、岭博科技（北京）有限公司、理光（中国）投资有限公司、科大讯飞股份有限公司、精华教育科技股份有限公司、江苏银行股份有限公司、佳能（中国）有限公司、济南中维世纪科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、淮南市银泰软件科技有限公司、湖北三新文化传媒有限公司、合肥奇乐网络科技有限公司、杭州伊柯夫科技有限公司、杭州雄伟科技开发股份有限公司、杭州汇点网络科技有限公司、杭州恒生数字设备科技有限公司、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、汉王科技股份有限公司、哈尔滨伟成科技有限公司、国核电力规划设计研究院有限公司、桂林佳朋信息科技有限公司、广州安网通信技术有限公司、广联达科技股份有限公司、帆软软件有限公司、东方雨虹民用建材有限责任公司、戴尔（中国）有限公司、成都卓越远扬信息技术有限公司、成都今网科技有限公司、成都瀚维特科技

有限公司、成都飞鱼星科技股份有限公司、贝尔金国际有限公司、北京中创视讯科技有限公司、北京中成科信科技发展有限公司、北京雪迪龙科技股份有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京我知科技有限公司、北京网康科技有限公司、北京通达志成科技有限公司、北京通达信科科技有限公司、北京天恒昕业科技发展有限公司、北京阔阔同创工贸有限公司、北京世纪超星信息技术发展有限责任公司、北京勤云科技发展有限公司、北京汉邦高科数字技术股份有限公司、北京百卓网络技术有限公司、北大医疗信息技术有限公司、安徽晶奇网络科技股份有限公司、ZIONCOM（香港）科技有限公司、TCL 商用信息科技（惠州）有限责任公司、宝创科技、帝国软件、华夏 ERP、乘风原创程序、深圳好生意网络工作室、zzcms、XnSoft、The PHP Group、The Apache Software Foundation、Sindoh (China) Marketing Co. Ltd、Jeeplus、Hancom、DD-WRT 和 COVID19-TMS 。

本周，CNVD 发布了《关于 SonarQube 系统存在未授权访问漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7041

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、北京数字观星科技有限公司、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、恒安嘉新（北京）科技股份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、北京信联科汇科技有限公司、贵州多彩宝互联网服务有限公司、南京树安信息技术有限公司、杭州迪普科技股份有限公司、河南灵创电子科技有限公司、山东云天安全技术有限公司、长春嘉诚信息技术股份有限公司、重庆都会信息科技有限公司、山东泽鹿安全技术有限公司、快页信息技术有限公司、北京安帝科技有限公司、浙江木链物联网科技有限公司、京东云安全、浙江大华技术股份有限公司、南京众智维信息科技有限公司、河南信安世纪科技有限公司、北京网御星云信息技术有限公司、广州易东信息安全技术有限公司、山东港口科技集团烟台有限公司、杭州天谷信息科技有限公司、福建省海峡信息技术有限公司、山东新潮信息技术有限公司、北京天地和兴科技有限公司、北京远禾科技有限公司、浙江大学控制科学与工程学院、天津偕行科技有限公司、广州安亿信软件科技有限公司、北方实验室（沈阳）股份有限公司、江苏云天网络安全技术有限公司、内蒙古洞明科技有限公司、北京惠而特科技有限公司、北京水木羽林科技有限公司、中资网络信息安全科技有限公司、博智安全科技股份有限公司、四川博恩信息技术有限公司、北京机沃科技有限公司、北京华云安信息技术有限公司及其他个人白帽子向 CNVD 提交了 10498 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）和上海交大向 CNVD 共享的白帽子报送的 8293 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）	3950	3950
斗象科技（漏洞盒子）	3673	3673
上海交大	670	670
北京神州绿盟科技有限公司	423	2
北京奇虎科技有限公司	287	0
北京数字观星科技有限公司	266	0
哈尔滨安天科技集团股份有限公司	246	0
新华三技术有限公司	175	0
恒安嘉新（北京）科技股份公司	119	0
深信服科技股份有限公司	112	0
华为技术有限公司	63	0
天津市国瑞数码安全系统股份有限公司	59	0
北京天融信网络安全技术有限公司	21	21
南京联成科技发展股份有限公司	5	5
北京知道创宇信息技术有限公司	2	2
北京启明星辰信息安全技术有限公司	1	1
北京智游网安科技有限公司	1	1
杭州安恒信息技术股份有限公司	1	1
沈阳东软系统集成工	1	1

程有限公司		
腾讯安全云鼎实验室	1	1
北京华顺信安科技有限公司	185	1
北京信联科汇科技有限公司	140	140
贵州多彩宝互联网服务有限公司	122	122
中国电信股份有限公司网络安全产品运营中心	80	0
南京树安信息技术有限公司	62	62
杭州迪普科技股份有限公司	60	16
河南灵创电子科技有限公司	59	59
山东云天安全技术有限公司	47	47
长春嘉诚信息技术股份有限公司	40	40
重庆都会信息科技有限公司	38	38
山东泽鹿安全技术有限公司	36	36
西门子（中国）有限公司	36	0
快页信息技术有限公司	20	20
北京安帝科技有限公司	20	20
浙江木链物联网科技有限公司	20	20
亚信科技（成都）有限公司	18	0

京东云安全	15	15
浙江大华技术股份有限公司	13	13
南京众智维信息科技有限公司	10	10
河南信安世纪科技有限公司	10	10
北京网御星云信息技术有限公司	9	9
广州易东信息安全技术有限公司	7	7
山东港口科技集团烟台有限公司	7	7
杭州天谷信息科技有限公司	6	6
福建省海峡信息技术有限公司	5	5
山东新潮信息技术有限公司	3	3
北京天地和兴科技有限公司	3	3
北京远禾科技有限公司	3	3
浙江大学控制科学与工程学院	2	2
天津偕行科技有限公司	2	2
广州安亿信软件科技有限公司	2	2
北方实验室（沈阳）股份有限公司	1	1
江苏云天网络安全技术有限公司	1	1
内蒙古洞明科技有限公司	1	1

北京惠而特科技有限公司	1	1
北京水木羽林科技有限公司	1	1
中资网络信息安全科技有限公司	1	1
博智安全科技股份有限公司	1	1
四川博恩信息技术有限公司	1	1
北京机沃科技有限公司	1	1
北京华云安信息技术有限公司	1	1
CNCERT 北京分中心	9	9
CNCERT 河北分中心	3	3
CNCERT 宁夏分中心	3	3
CNCERT 山东分中心	3	3
个人	1424	1424
报送总计	12608	10498

本周漏洞按类型和厂商统计

本周，CNVD 收录了 585 个漏洞。WEB 应用 246 个，应用程序 163 个，网络设备（交换机、路由器等网络端设备）89 个，智能设备（物联网终端设备）36 个，操作系统 31 个，安全产品 18 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	246
应用程序	163
网络设备（交换机、路由器等网络端设备）	89
智能设备（物联网终端设备）	36
操作系统	31
安全产品	18
数据库	2

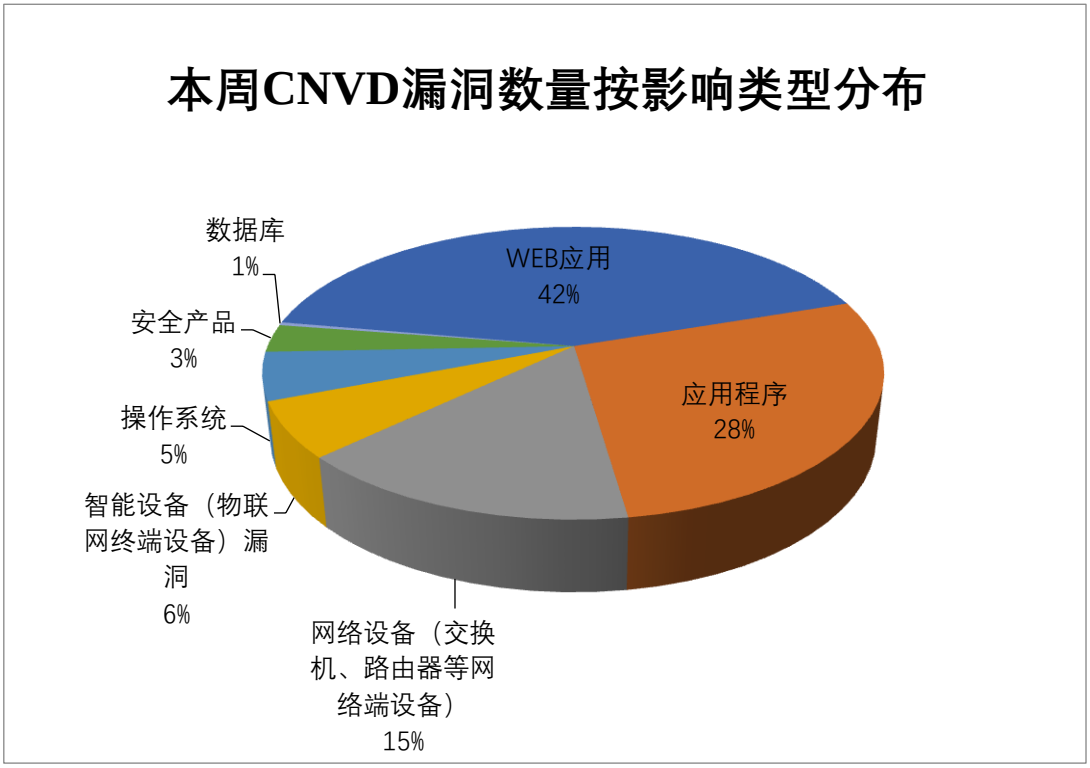

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Siemens、IBM 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	D-Link	32	6%
2	Siemens	26	5%
3	IBM	24	4%
4	Microsoft	24	4%
5	XnSoft	23	4%
6	Wildbit	14	2%
7	JetBrains	13	2%
8	Bandisoft	12	2%
9	爱青檬 CMS	11	2%
10	其他	406	69%

本周行业漏洞收录情况

本周，CNVD 收录了 58 个电信行业漏洞，11 个移动互联网行业漏洞，20 个工控行业漏洞（如下图所示）。其中，“Zoho ManageEngine Network Configuration Manager SQL 注入漏洞、Siemens SIMATIC PCS 7 和 SIMATIC WinCC 路径遍历漏洞（CNVD-2021-89422）、Zoho ManageEngine Desktop Central 远程代码执行漏洞（CNVD-2021-

88243）”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/

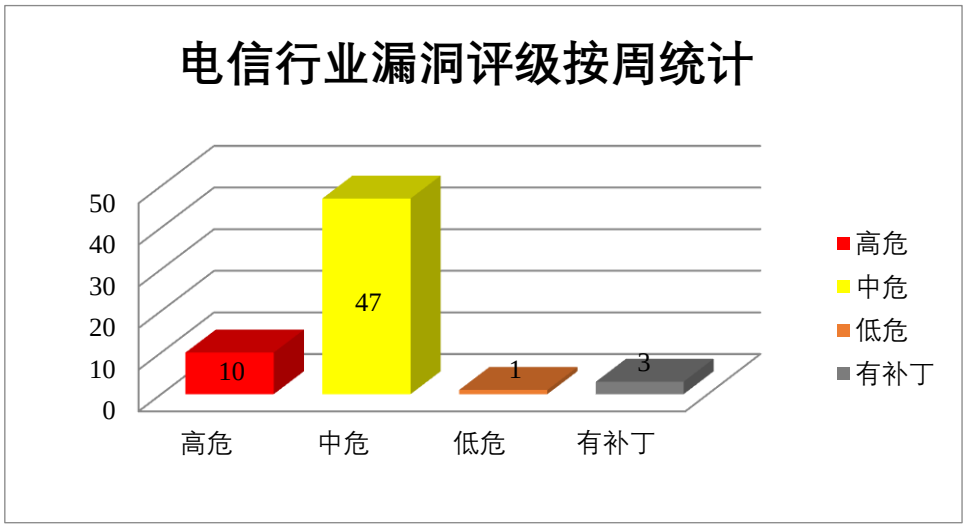

图 3 电信行业漏洞统计

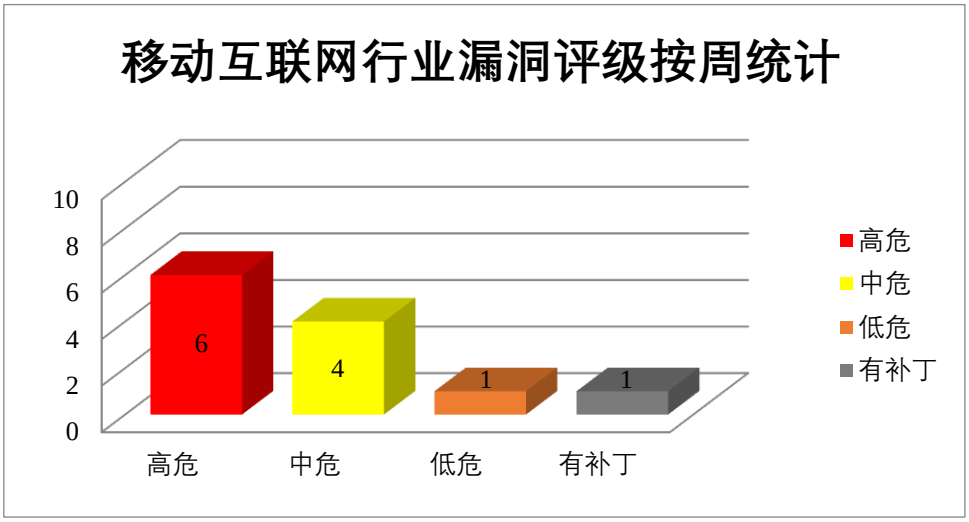

图 4 移动互联网行业漏洞统计

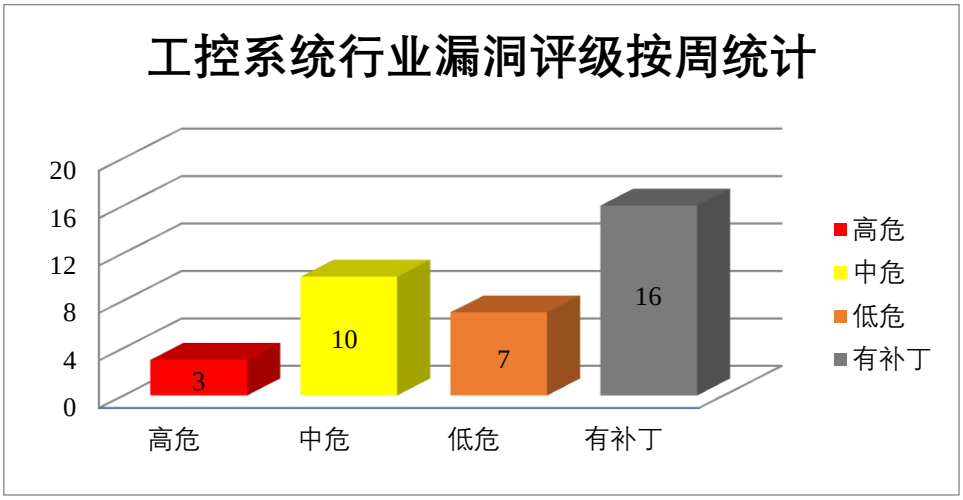

图 5 工控系统行业漏洞统计

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 Reader（也被称为 Acrobat Reader）是 Adobe 公司开发的一款 PDF 文件阅读软件。Adobe Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。Adobe InCopy 是 Adobe 公司推出的专业文字处理程序，与 Adobe InDesign 集成在一起。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Adobe InCopy 内存越界访问漏洞（CNVD-2021-87304）、Adobe Acrobat/Reader 空指针解引用漏洞（CNVD-2021-87305、CNVD-2021-87307、CNVD-2021-87306、CNVD-2021-87308、CNVD-2021-87309、CNVD-2021-87310）、Adobe Acrobat/Reader 释放后重用漏洞（CNVD-2021-87312）。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-2021-87304
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87305
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87307
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87306
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87308
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87309
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87310
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87312

2、 Microsoft 产品安全漏洞

Microsoft Windows Active Directory 是美国微软（Microsoft）公司的一个负责架构

中大型网络环境的集中式目录管理服务。Microsoft Windows Installer 是美国微软（Microsoft）公司的 Windows 操作系统的一个组件。为安装和卸载软件提供了标准基础。Microsoft Windows Media Foundation 是适用于 Windows 的下一代多媒体平台。Microsoft Windows Diagnostic Hub 是美国微软（Microsoft）公司的一款应用程序。它不仅仅是任务管理器，也是设备诊断中心。此应用程序将 Windows 开发人员工具与 UWP 功能相结合，以获取新信息和功能。Microsoft Windows NTFS 是美国微软（Microsoft）公司的一个为计算机文件服务的文件系统。Microsoft Dynamics 365 是一套适用于跨国企业的 ERP 业务解决方案。Microsoft Windows Fastfat Driver 是美国微软（Microsoft）公司的一个完整的文件系统，它解决了各种问题，例如在磁盘上存储数据、与缓存管理器交互以及处理各种 I/O 操作，例如文件创建、对文件执行读/写、设置文件信息以及对文件系统执行控制操作。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，在目标主机上执行代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Active Directory 权限提升漏洞、Microsoft Windows Installer 权限提升漏洞、Microsoft Windows Media Foundation 远程代码执行漏洞、Microsoft Windows Diagnostic Hub 权限提升漏洞、Microsoft Windows NTFS 权限提升漏洞、Microsoft Dynamics 365 远程代码执行漏洞、Microsoft Windows NTFS 远程代码执行漏洞、Microsoft Windows Fastfat Driver 权限提升漏洞。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-2021-87324
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87329
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87326
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87325
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87333
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87332
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87331
https://www.cnvd.org.cn/flaw/show/CNVD-2021-87330

3、IBM 产品安全漏洞

IBM Security Access Manager 是美国 IBM 公司的一款应用于信息安全管理的产品。IBM Sterling Secure Proxy 是一个用于确保组织非保护区（DMZ）中文件安全传输的应用程序代理。IBM Ts7700 是美国 Ibm 公司的一款大型机虚拟磁带解决方案。用于优化数据安全性和业务连续性。IBM AIX 是美国 IBM 公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。IBM QRadar User Behavior Analytics（UBA）是美国 IBM 公司的一款用户行为分析软件。IBM QRadar Advisor w

ith Watson 是美国 IBM 公司的一套安全威胁分析解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞解密高度敏感的信息，从系统发送未经授权的请求，进而探测系统内网，执行任意命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Security Access Manager 加密问题漏洞、IBM Sterling Secure Proxy 服务器端请求伪造漏洞、IBM TS7700 授权问题漏洞、IBM AIX 拒绝服务漏洞（CNVD-2021-88195、CNVD-2021-88194）、IBM Maximo Asset Management CSV 注入漏洞（CNVD-2021-88198）、IBM QRadar User Behavior Analytics 跨站请求伪造漏洞、IBM QRadar Advisor with Watson 跨站脚本漏洞。其中，“IBM TS7700 授权问题漏洞、IBM Maximo Asset Management CSV 注入漏洞（CNVD-2021-88198）”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-2021-88180

https://www.cnvd.org.cn/flaw/show/CNVD-2021-88181

https://www.cnvd.org.cn/flaw/show/CNVD-2021-88191

https://www.cnvd.org.cn/flaw/show/CNVD-2021-88195

https://www.cnvd.org.cn/flaw/show/CNVD-2021-88194

https://www.cnvd.org.cn/flaw/show/CNVD-2021-88198

https://www.cnvd.org.cn/flaw/show/CNVD-2021-88201

https://www.cnvd.org.cn/flaw/show/CNVD-2021-88947

4、Siemens 产品安全漏洞

SIMATIC PCS 7 是一套过程控制系统。SIMATIC WinCC 是一套自动化的数据采集与监控（SCADA）系统。Siemens Climatix Pol909 是德国西门子（Siemens）公司的一个智能网络模块。Capital VSTAR 是一个完整的解决方案。Nucleus NET 模块集成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。Nucleus RTOS 是一种基于微内核的实时操作系统。Siemens Nucleus ReadyStart 是一个捆绑式解决方案。用于加速完整系统的快速启动并提供丰富的板级支持包（Bsp）。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敏感数据，导致拒绝服务条件等。

CNVD 收录的相关漏洞包括：Siemens SIMATIC PCS 7 和 SIMATIC WinCC 路径遍历漏洞（CNVD-2021-89422、CNVD-2021-89425）、Siemens Climatix POL909 (AWM)信息泄露漏洞、Siemens SIMATIC PCS 7 和 SIMATIC WinCC 日志信息泄露漏洞、多款 Siemens 产品缓冲区溢出漏洞（CNVD-2021-89441、CNVD-2021-89442）、多款 Siemens 产品越界读取漏洞 、Siemens Nucleus ReadyStart 拒绝服务漏洞。其中，“Siemens SIMATIC PCS 7 和 SIMATIC WinCC 路径遍历漏洞（CNVD-2021-89422）”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-2021-89422

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89425

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89433

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89451

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89441

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89442

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89443

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89423

5、WildBit Viewer 缓冲区溢出漏洞（CNVD-2021-88229）

WildBit Viewer 是一款带有幻灯片放映和编辑器的小巧型图像查看器。本周，Wild Bit Viewer 被披露存在缓冲区溢出漏洞。攻击者可通过特制 tga 文件利用该漏洞导致拒绝服务。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-2021-88229

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-2021-88233	Zoho ManageEngine Patch Connect Plus 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.manageengine.com/sccm-third-party-patch-management/kb/unauthenticated-remote-code-execution.html
CNVD-2021-88202	Cron Utils 代码注入漏洞	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/jmrozanec/cron-utils/commit/cfd2880f80e62ea74b92fa83474c2aabdb9899da
CNVD-2021-88243	Zoho ManageEngine Desktop Central 远程代码执行漏洞（CNVD-2021-88243）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.manageengine.com/products/desktop-central/unauthenticated-command-injection-vulnerability.html
CNVD-2021-89057	JetBrains Hub 认证限制机	高	厂商已发布了漏洞修复程序，

	制绕过漏洞		请及时关注更新：https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/
CNVD-2021-89447	Aruba Instant 命令注入漏洞（CNVD-2021-89447）	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.cybersecurity-help.cz/vdb/SB2021100720
CNVD-2021-88235	Zoho ManageEngine ADAudit Plus 任意文件写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://pitstop.manageengine.com/portal/en/community/topic/fix-released-for-a-vulnerability-in-manageengine-adaudit-plus
CNVD-2021-89058	JetBrains TeamCity 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://blog.jetbrains.com/blog/2021/11/08/jetbrains-security-bulletin-q3-2021/
CNVD-2021-88249	ZOHO ManageEngine ADSelfService Plus 远程代码执行漏洞（CNVD-2021-88249）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6104-released
CNVD-2021-89431	Siemens Mendix 不正确授权漏洞	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-779699.pdf
CNVD-2021-88252	Zoho ManageEngine ADSelfService Plus 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.manageengine.com/products/self-service-password/release-notes.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致拒绝服务等。此外，Microsoft、IBM、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞解密高度敏感的信息，从系统发送未经授权的请求，进而探测系统内网，提升权限，执行任意命令，导致拒绝服务等。另外，WildBit Viewer 被披露存在缓冲区溢出漏洞。攻击者可通过特制 tga 文件利用该漏洞导致拒绝服务。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、AyaCMS 跨站请求伪造漏洞

验证描述

AyaCMS 是一个极其简单且自由的开源 Php 建站系统。

AyaCMS 存在跨站请求伪造漏洞，该漏洞源于软件在更改管理员密码的操作中缺少对于跨站请求伪造的检查。攻击者可利用该漏洞更改管理员密码或其他未指明的影响。

验证信息

POC 链接：https://github.com/loadream/AyaCMS/issues/1

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-88725

信息提供者

恒安嘉新（北京）科技股份公司

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. 英特尔曝出多款处理器存在高危漏洞

英特尔公布了三个影响范围广泛的自家处理器高危漏洞，能够允许攻击者和恶意软件在设备系统上获得增强权限。

参考链接：https://www.bleepingcomputer.com/news/security/high-severity-bios-flaws-affect-numerous-intel-processors/

2. 索尼 PS5 曝两个内核漏洞，可用来窃取根密钥

继 Xbox 主机曝出外挂后，索尼 PS5 也在同一日曝出两个内核漏洞，攻击者利用这两个漏洞窃取了 PS5 的根密钥。

参考链接：https://www.freebuf.com/vuls/304846.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