

信息安全漏洞周报

2021 年 11 月 01 日-2021 年 11 月 07 日

2021 年第 44 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 527 个，其中高危漏洞 127 个、中危漏洞 340 个、低危漏洞 60 个。漏洞平均分为 5.63。本周收录的漏洞中，涉及 0day 漏洞 253 个（占 48%），其中互联网上出现“Spotweb 跨站脚本漏洞、Gila CMS SQL 注入漏洞（CNVD-2021-84282）”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 13110 个，与上周（14569 个）环比减少 10%。

CNVD收录漏洞近10周平均分分布图

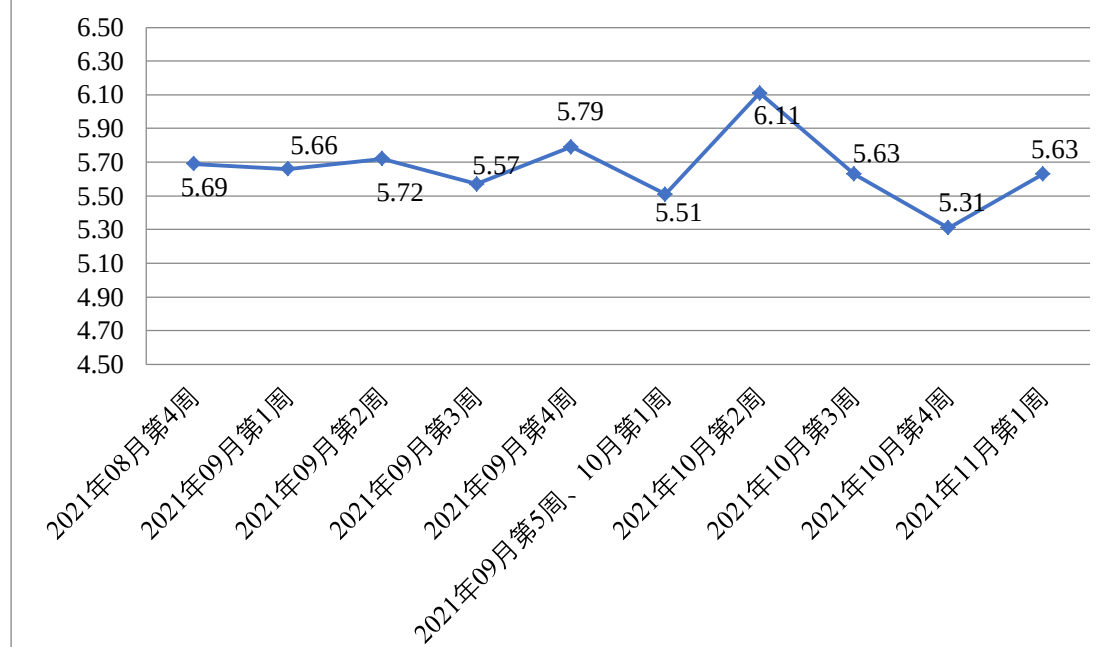


图 1 CNVD 收录漏洞近 10 周平均分分布图

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 25 起，向基础电信企业通报漏洞事件 24 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 754 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 151 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 72 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、中国运载火箭技术研究所、郑州博雅讯科技有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、新都（青岛）办公系统有限公司、西安九佳易信息资讯有限公司、西安邦易网络科技有限公司、微软（中国）有限公司、通力电梯有限公司、天津天堰科技股份有限公司、松下电器（中国）有限公司、世邦通信股份有限公司、石家庄捷搜网络科技有限公司、沈阳点动科技有限公司、深圳市迅捷通信技术有限公司、深圳市蓝凌软件股份有限公司、深圳市合信自动化技术有限公司、深圳市富士智能系统有限公司、深圳市必联电子有限公司、深圳零零无限科技有限公司、上海卓卓网络科技有限公司、上海井星信息科技有限公司、上海斐讯数据通信技术有限公司、上海安达通信息安全技术股份有限公司、山西企凝信息科技有限公司、山东领图信息科技股份有限公司、润申信息科技（上海）有限公司、瑞纳智能设备股份有限公司、普联技术有限公司、欧姆龙自动化（中国）有限公司、南京九则软件科技有限公司、南昌北创科技发展有限公司、咪咕视讯科技有限公司、龙采科技集团有限责任公司、联奕科技股份有限公司、廊坊市极致网络科技有限公司、珠海金山办公软件有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、洪湖尔创网联信息技术有限公司、杭州盈高科技有限公司、杭州贝腾科技有限公司、海湾安全技术有限公司、桂林崇胜网络科技有限公司、广州易全信息科技有限公司、广州好象科技有限公司、福州网钛软件科技有限公司、戴尔（中国）有限公司、大连龙采科技开发有限公司、大连菲尔科技有限公司、成都万江港利科技股份有限公司、北京卓软在线信息技术有限公司、北京亚鸿世纪科技发展有限公司、北京星网锐捷网络技术有限公司、北京网易有道计算机系统有限公司、北京网瑞达科技有限公司、北京通达志成科技有限公司、北京上元信安技术有限公司、北京城市联盟科技有限公司、北京碧海威科技有限公司、安徽青柿信息科技有限公司、帝国软件、京瓷株式会社、施耐德（Schneider Electric）、梦想 CMS、zzzcms、YIXUNCMS、ToTolink、TaoCMS、SoftMaker、OpenSSL、FLIF、Bandisoft 和 aqmcms。



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、北京奇虎科技有限公司、哈尔滨安天科技集团股份有限公司、北京数字观星科技有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。广东蓝爵网络安全技术股份有限公司、山东云天安全技术有限公司、新疆海狼科技有限公司、杭州海康威视数字技术股份有限公司、贵州多彩宝互联网服务有限公司、南京众智维信息科技有限公司、河南灵创电子科技有限公司、北京信联科汇科技有限公司、北京华云安信息技术有限公司、长春嘉诚信息技术股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、安徽长泰科技有限公司、重庆都会信息科技有限公司、北京山石网科信息技术有限公司、快页信息技术有限公司、星云博创科技有限公司、北京安帝科技有限公司、杭州迪普科技股份有限公司、南京树安信息技术有限公司、北京惠而特科技有限公司、内蒙古云科数据服务股份有限公司、北京远禾科技有限公司、思而听网络科技有限公司、河南信安世纪科技有限公司、浙江木链物联网科技有限公司、上海纽盾科技股份有限公司、云南南天电子信息产业股份有限公司、福建省海峡信息技术有限公司、苏州棱镜七彩信息科技有限公司、北京网御星云信息技术有限公司、广州安亿信软件科技有限公司、江苏耘和计算机工程有限公司、北方实验室（沈阳）股份有限公司、江苏智慧安全可信技术研究院、奇安信科技集团股份有限公司、山石网科通信技术股份有限公司、杭州美创科技有限公司、北京水木羽林科技有限公司、内蒙古洞明科技有限公司、平安银河实验室、郑州天宇鸿图电子科技有限公司郑州天宇鸿图电子科技有限公司、中移（杭州）信息技术有限公司及其他个人白帽子向 CNVD 提交了 13110 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 8879 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）	5427	5427
斗象科技（漏洞盒子）	3076	3076
上海交大	376	376
北京神州绿盟科技有限公司	323	13
北京奇虎科技有限公司	308	0
哈尔滨安天科技集团股份有限公司	250	0
北京数字观星科技有限公司	207	0
新华三技术有限公司	205	0
深信服科技股份有限公司	128	0
恒安嘉新（北京）科技股份公司	123	0
华为技术有限公司	73	0
北京启明星辰信息安全技术有限公司	65	8

远江盛邦（北京）网络安全科技股份有限公司	61	61
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	44	44
西安四叶草信息技术有限公司	21	21
南京联成科技发展股份有限公司	17	17
杭州安恒信息技术股份有限公司	11	11
沈阳东软系统集成工程有限公司	6	6
北京知道创宇信息技术有限公司	3	0
腾讯安全云鼎实验室	1	1
内蒙古奥创科技有限公司	1	1
广东蓝爵网络安全技术股份有限公司	489	489
联想集团	200	0
山东云天安全技术有限公司	175	175
北京华顺信安科技有限公司	162	0
新疆海狼科技有限公司	123	123
杭州海康威视数字技术股份有限公司	122	122
贵州多彩宝互联网服务有限公司	122	122
南京众智维信息科技有限公司	122	122
河南灵创电子科技有限公司	110	110
北京信联科汇科技有限公司	105	105
北京华云安信息技术有限公司	80	80
长春嘉诚信息技术股份有限公司	58	58
北京云科安信科技有限公司（Seraph 安全实验室）	38	38
安徽长泰科技有限公司	33	33
亚信科技（成都）有限公司	31	0
重庆都会信息科技有限公司	30	30
北京山石网科信息技术有限公司	27	27
快页信息技术有限公司	25	25
星云博创科技有限公司	23	23
北京安帝科技有限公司	21	21
杭州迪普科技股份有限公司	16	2
南京树安信息技术有限公司	15	15
北京惠而特科技有限公司	13	13
内蒙古云科数据服务股份有限公司	11	11

北京远禾科技有限公司	11	11
思而听网络科技有限公司	9	9
河南信安世纪科技有限公司	8	8
浙江木链物联网科技有限公司	6	6
上海纽盾科技股份有限公司	4	4
云南南天电子信息产业股份有限公司	4	4
福建省海峡信息技术有限公司	3	3
苏州棱镜七彩信息科技有限公司	3	3
北京网御星云信息技术有限公司	3	3
广州安亿信软件科技有限公司	3	3
江苏耘和计算机工程有限公司	3	3
北方实验室（沈阳）股份有限公司	3	3
江苏智慧安全可信技术研究院	2	2
奇安信科技集团股份有限公司	2	2
山石网科通信技术股份有限公司	2	2
杭州美创科技有限公司	2	2
北京水木羽林科技有限公司	2	2
内蒙古洞明科技有限公司	2	2
平安银河实验室	2	2
郑州天宇鸿图电子科技有限公司郑州天宇鸿图电子科技有限公司	1	1
中移（杭州）信息技术有限公司	1	1
CNCERT 青海分中心	5	5
CNCERT 贵州分中心	1	1
个人	2222	2222
报送总计	15240	13110

本周漏洞按类型和厂商统计

本周，CNVD 收录了 527 个漏洞。应用程序 203 个，WEB 应用 181 个，网络设备（交换机、路由器等网络端设备）63 个，操作系统 34 个，智能设备（物联网终端设备）33 个，安全产品 10 个，数据库 3 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	203
WEB 应用	181
网络设备（交换机、路由器等网络端设备）	63
操作系统	34
智能设备（物联网终端设备）	33
安全产品	10
数据库	3

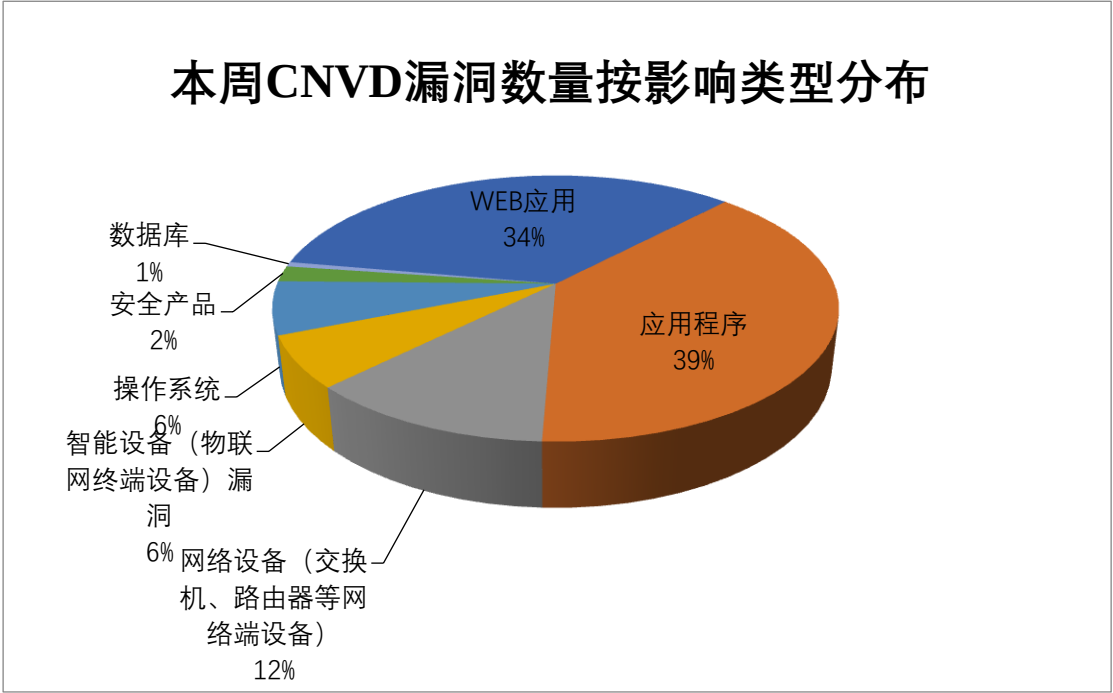


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Huawei、GPAC、Microsoft 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	Huawei	30	6%
2	GPAC	24	5%
3	Microsoft	21	4%
4	Adobe	20	4%
5	IBM	20	4%
6	Fortinet	19	4%
7	AUVESY	17	3%
8	INFRAWARE	17	3%
9	Zammad	14	3%
10	其他	345	64%



本周行业漏洞收录情况

本周，CNVD 收录了 53 个电信行业漏洞，5 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“FATEK Automation WinProladder 越界读取漏洞、多种 NETGEAR 交换机存在授权问题漏洞”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/>

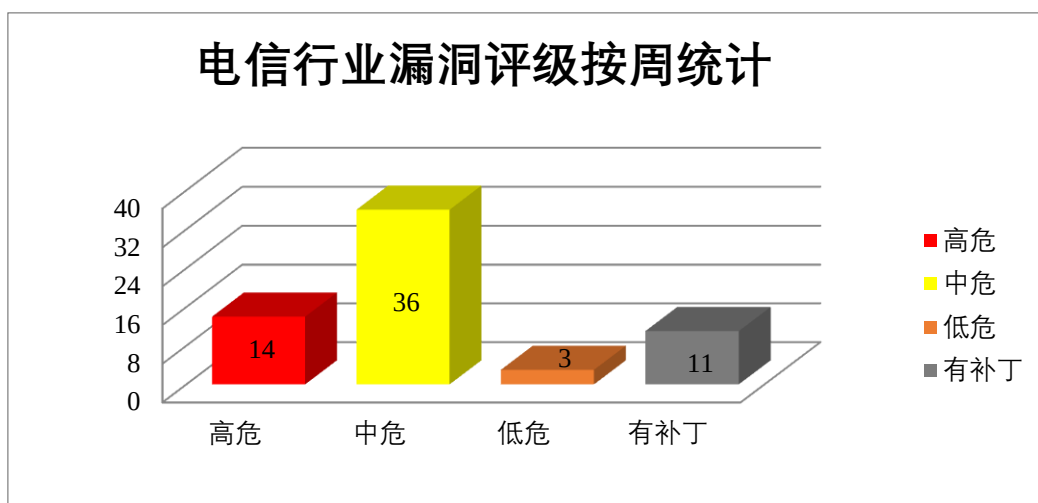


图 3 电信行业漏洞统计

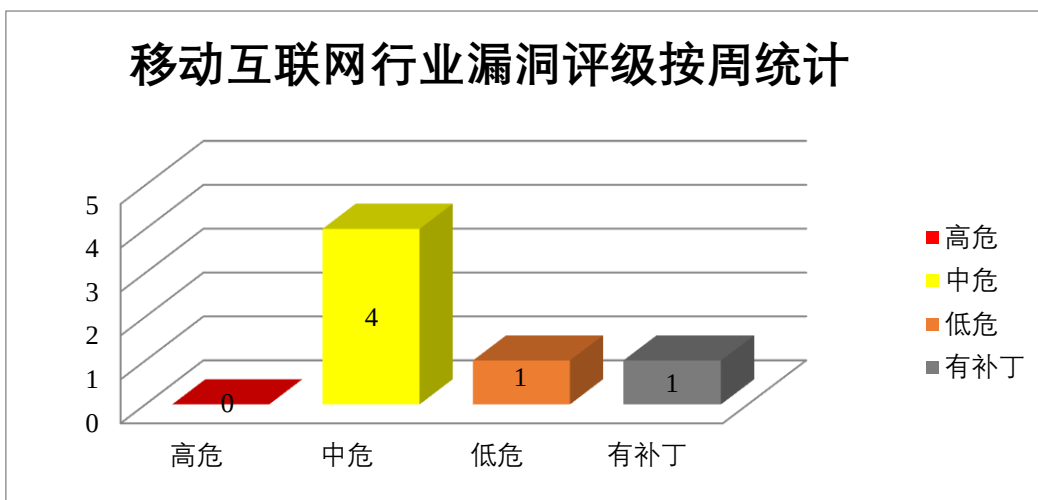


图 4 移动互联网行业漏洞统计

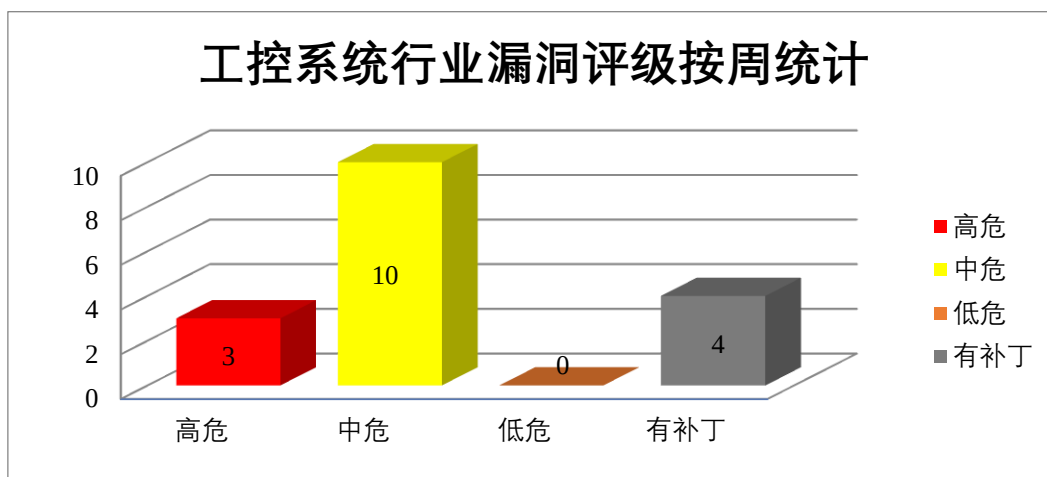


图 5 工控系统行业漏洞统计

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、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 Imanager NetEco 是一款专业的能源基础设施管理平台。Huawei FusionCompute 是一款计算机虚拟化引擎。该产品提供虚拟资源管理器（VRM）和计算节点代理（CNA）等。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞提升权限，导致系统重新启动，执行恶意代码等。

CNVD 收录的相关漏洞包括：Huawei Emui 和 Magic UI 代码注入漏洞、Huawei Emui 和 Magic UI 竞争条件漏洞（CNVD-2021-83527）、Huawei Emui 和 Magic UI 篡改内核漏洞（CNVD-2021-83525、CNVD-2021-83528）、Huawei Emui 和 Magic UI 内核崩溃漏洞、Huawei iManager NetEco 不正确签名管理漏洞、Huawei Emui 和 Magic UI 内存越界访问漏洞、Huawei FusionCompute 产品命令注入漏洞。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-2021-83524>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83528>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83527>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83525>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83535>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83540>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83538>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83544>

2、Adobe 产品安全漏洞

Adobe Premiere Elements 是一款视频编辑软件应用程序。Adobe Animate 是一款多媒体创作和计算机动画程序。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Premiere Elements 内存越界访问漏洞（CNVD-2021-82408、CNVD-2021-82411、CNVD-2021-82407、CNVD-2021-82410、CNVD-2021-82409）、Adobe Animate 越界写入漏洞（CNVD-2021-84298、CNVD-2021-84301、CNVD-2021-84300）。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-2021-82408>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82407>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82411>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82410>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82409>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-84298>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-84301>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-84300>

3、IBM 产品安全漏洞

IBM Sterling B2B Integrator 是一个交易引擎，是一套根据您的业务需求运行您定义和管理的流程的组件。IBM Sterling File Gateway 是一款用于在内部和外部合作伙伴之间传输文件的应用程序，可让您更加安全可靠地与贸易伙伴进行文件传输。IBM Data Risk Manager 是一款数据风险管理器。IBM Jazz Team Server 是一个应用服务器。提供了基础服务，这些服务使一组工具可以作为单个逻辑服务器一起工作，并且包括提供工具特定功能的任意数量的 Jazz Team Server Extensions。IBM InfoSphere Information Server 是一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞执行从网站信任的用户传输的恶意和未经授权的操作，解密高度敏感的信息，导致拒绝其他用户的服务等。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2021-82418）、IBM Sterling B2B Integrator 跨站请求伪造漏洞（CNVD-2021-82420）、IBM Sterling File Gateway 授权问题漏洞、IBM Sterling File Gateway 拒绝服务漏洞、IBM Sterling File Gateway 代码问题漏洞、IBM Data Risk Manager 加密问题漏洞、IBM Jazz Team Server 权限提升漏洞、IBM InfoSphere Information Server 跨站请求伪造漏洞（CNVD-2021-84239）。其中，“IBM Sterling B2B Integrator SQL 注入漏洞（CNVD-2021-82418）”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-2021-82418>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82420>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82424>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82423>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-82426>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83787>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-84222>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-84239>

4、NETGEAR 产品安全漏洞

NETGEAR 是美国网件（Netgear）公司的一款路由器。连接两个或多个网络的硬件设备，在网络间起网关的作用。GC108P 等都是智能交换机产品。Netgear genie 是一个将自己呈现为仪表板的程序。NETGEAR JNR1010 等都是一款无线路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞执行系统命令，导致恶意文件创建以及权限提升等。

CNVD 收录的相关漏洞包括：NETGEAR 代码注入漏洞、多款 NETGEAR 设备命令注入漏洞（CNVD-2021-83557、CNVD-2021-83563）、NETGEAR 多款产品命令注入漏洞、NETGEAR 多款智能交换机存在输入验证错误漏洞、多种 NETGEAR 交换机存在授权问题漏洞、NETGEAR genie 代码问题漏洞、多款 NETGEAR 产品授权问题漏洞（CNVD-2021-83565）。其中，“NETGEAR 代码注入漏洞、多种 NETGEAR 交换机存在授权问题漏洞”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-2021-83558>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83557>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83563>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83562>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83561>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83559>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83566>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-83565>

5、Tenda AC-10U 缓冲区溢出漏洞

Tenda AC-10U 是中国腾达（Tenda）公司的一款无线路由器。本周，Tenda AC-10U AC1200 路由器被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过 goform/SetSysTimeCfg 的 timeZone 参数执行任意代码。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-2021-84224>

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-2021-81954	Zammad 远程代码执行漏洞 (CNVD-2021-81954)	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://zammad.com/en/advisories/zaa-2021-14
CNVD-2021-81962	Draytek VigorConnect 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: https://www.draytek.com/products/vigorconnect/
CNVD-2021-81963	Draytek VigorConnect 任意文件上传和目录遍历漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://www.draytek.com/products/vigorconnect/
CNVD-2021-82412	Adobe Premiere Pro 内存越界访问漏洞 (CNVD-2021-82412)	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/premiere_pro/apsb21-67.html
CNVD-2021-82413	Adobe Premiere Pro 内存越界访问漏洞 (CNVD-2021-82413)	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/premiere_pro/apsb21-67.html
CNVD-2021-82928	AUVESY Versiondog 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.my.versiondog.com/home-en.html
CNVD-2021-82941	AUVESY Versiondog 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.my.versiondog.com/home-en.html
CNVD-2021-82958	Microsoft Windows/Windows Server 脚本引擎内存破坏漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34448
CNVD-2021-82961	Microsoft Windows/Windows Server 安全特性绕过漏洞 (CNVD-2021-82961)	高	厂商已发布了漏洞修复程序, 请及时关注更新: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-3757

CNVD-2021-82965	Microsoft Exchange Server 权限提升漏洞（CNVD-2021-82965）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34523
-----------------	---	---	--

小结：本周，Huawei 产品被披露存在多个漏洞，攻击者可利用该漏洞提升权限，导致系统重新启动，执行恶意代码等。此外，Adobe、IBM、NETGEAR 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞执行从网站信任的用户传输的恶意和未经授权的操作，执行系统命令，解密高度敏感的信息，导致恶意文件创建以及权限提升等。另外，AC1200 路由器被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过 goform/SetSysTimeCfg 的 timeZone 参数执行任意代码。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、Gila CMS SQL 注入漏洞（CNVD-2021-84282）

验证描述

Gila CMS 是一套基于 PHP 和 MySQL 的开源内容管理系统(CMS)。

Gila CMS 1.11.4 版存在 SQL 注入漏洞，攻击者可通过/src/core/controllers/cm.php 中的\$_GET 参数利用该漏洞进行 SQL 注入攻击。

验证信息

POC 链接：<https://github.com/GilaCMS/gila/issues/50>

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2021-84282>

信息提供者

恒安嘉新（北京）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. CISA 发布 306 个已知漏洞目录，命令联邦机构及时修补

11 月 5 日，美国网络安全与基础设施安全局（CISA）发布了 306 个被积极利用的漏洞目录，并配套出台了一系列具有强约束力的操作指令，命令美国联邦机构在特定时间范围内及时修补这些漏洞。

参考链接：<https://www.freebuf.com/news/303783.html>

2. 高危漏洞曝光半年之久，超 50% 的 GitLab 服务器仍未修复

据 Rapid7 发布的报告显示，半年多以前已经披露的一个高危漏洞，直到现在竟然还有一多半的 GitLab 服务器仍然没有进行修复。犯罪分子完全可以利用这个已知的漏洞发起网络攻击。

参考链接：https://www.bleepingcomputer.com/news/security/over-30-000-gitlab-servers-still-unpatched-against-critical-bug/?_cf_chl_jschl_tk=__=39.MnHT7patmu9EIspvP3A2.pzZfkTaurQa6TmEyM5s-1636345077-0-gaNycGzNB_0

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