# 国家信息安全漏洞共享平台(CNVD)

# 信息安全漏洞周报

2021 年 08 月 30 日-2021 年 09 月 05 日

2021 年第 35 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 550 个，其中高危漏洞 168 个、中危漏洞 309 个、低危漏洞 73 个。漏洞平均分值为 5.66。本周收录的漏洞中，涉及 0day 漏洞 420 个（占 76%），其中互联网上出现“Remote Mouse 目录遍历漏洞、WordPress Duplicate Page 跨站脚本漏洞”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 12712 个，与上周（15481 个）环比减少 18%。

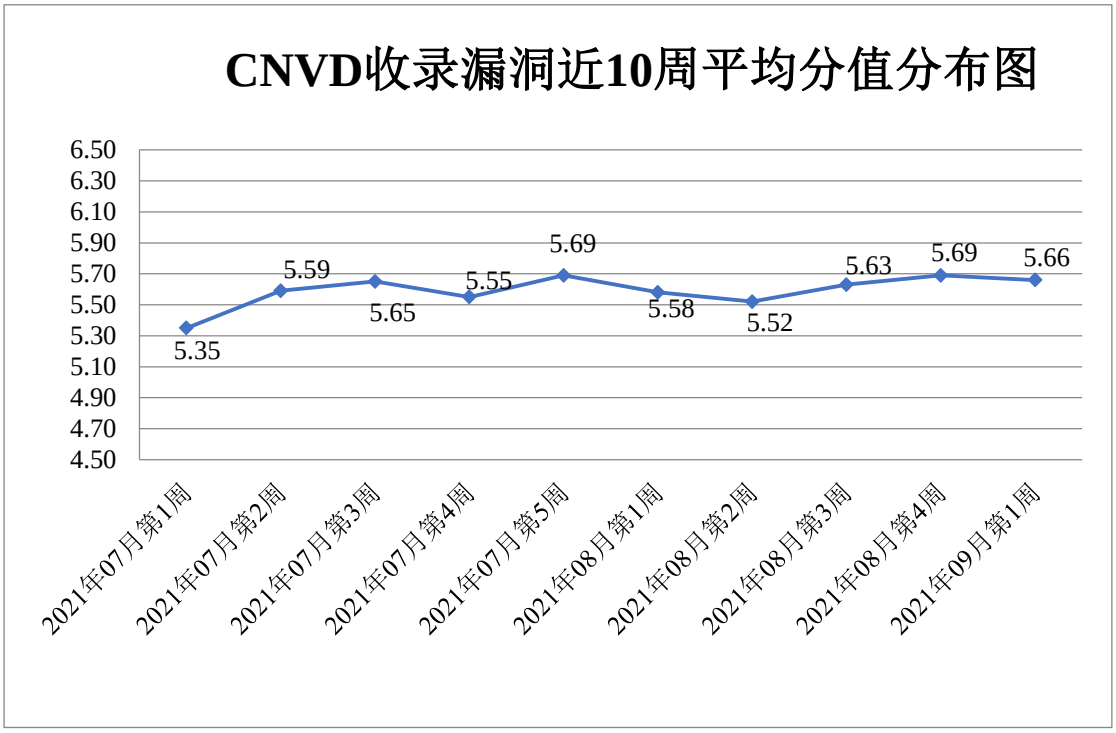


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 30 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 447 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 54 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 53 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、珠海新华通软件股份有限公司、重庆森鑫炬科技有限公司、众勤通信设备贸易（上海）有限公司、中山市星廷网络科技有限公司、中科博华信息科技有限公司、浙江网盛生意宝股份有限公司、浙江大华技术股份有限公司、长沙精博信息技术有限公司、友讯电子设备（上海）有限公司、西安昊博智能科技有限公司、西安启莱软件科技有限公司、西安华天协同信息技术有限公司、武汉雕龙数据科技有限公司、无锡信捷电气股份有限公司、微软（中国）有限公司、网件公司、天津亿通达科技发展有限公司、天津天堰科技股份有限公司、天津黑核科技有限公司、苏州思迪信息技术有限公司、苏州梦图地理信息系统有限责任公司、苏州科达科技股份有限公司、世邦通信股份有限公司、石家庄市征红网络科技有限公司、施耐德电气（中国）有限公司、深圳市腾讯计算机系统有限公司、深圳市思迅软件股份有限公司、深圳市深日科技有限公司、深圳市美科星通信技术有限公司、深圳市动力启航软件有限公司、深圳乐播科技有限公司、上海远丰信息科技（集团）有限公司、上海纽盾科技股份有限公司、上海穆云智能科技有限公司、上海国云信息科技有限公司、上海二三四五移动科技有限公司、上海顶想信息科技有限公司、上海冰峰计算机网络技术有限公司、上海碧海网络科技有限公司、上海艾泰科技有限公司、厦门四信通信科技有限公司、厦门狄耐克智能科技股份有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、日冲商业（北京）有限公司、任子行网络技术股份有限公司、普联技术有限公司、南大傲拓科技江苏有限公司、美满电子科技（Marvell）公司、龙采科技集团有限责任公司、联想（北京）有限公司、朗坤智慧科技股份有限公司、江西铭软科技有限公司、佳能（中国）有限公司、华硕电脑（上海）有限公司、华大半导体有限公司、杭州西软信息技术有限公司、哈尔滨伟成科技有限公司、广州酷狗计算机科技有限公司、广州佳蓝计算机软件有限公司、广州红帆科技有限公司、广州鼎成信息科技有限公司、广西金中软件集团有限公司、广东迪浪科技股份有限公司、福州网钛软件科技有限公司、福建福昕软件开发股份有限公司、佛山市顺德区天轴车料有限公司、大唐电信科技股份有限公司、成都龙兵科技有限公司、成都蓝海之星科技有限公司、郴州帝云网络科技有限公司、北京众智创世科技有限公司、北京中广上洋科技股份有限公司、北京中达信泰科技有限公司、北京中成科信科技发展有限公司、北京星网锐捷网络技术有限公司、北京网动网络科技股份有限公司、北京万维盈创科技发展有限公司、北京万户网络技术有限公司、北京通达信

科科技有限公司、北京停简单信息技术有限公司、北京神州数码云科信息技术有限公司、北京奇虎科技有限公司、北京南北天地科技股份有限公司、北京康智乐思网络科技有限公司、北京电音多多科技有限公司、北京辰信领创信息技术有限公司、北京百卓网络技术有限公司、傲拓科技股份有限公司、安徽青柿信息科技有限公司、帝国软件、智睿软件、狂雨小说 cms、站帮主 CMS、鱼跃 CMS、梦想 CMS、魅思视频系统、ZrLog、YIXUNCMS、The HDF Group、sikcms、Nitro、lzcms、Irfan Skiljan、Intego、HDF Group、Emerson、EasySNS、Bento4、BageCms、Apache 和 AKCMS。

## 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、新华三技术有限公司、北京神州绿盟科技有限公司、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。山东新潮信息技术有限公司、山东云天安全技术有限公司、联想集团、北京华云安信息技术有限公司、南京众智维信息科技有限公司、中国电信股份有限公司网络安全产品运营中心、北京山石网科信息技术有限公司、浙江木链物联网科技有限公司、河南灵创电子科技有限公司、北京信联科汇科技有限公司、内蒙古洞明科技有限公司、河南信安世纪科技有限公司、广东蓝爵网络安全技术股份有限公司、信联科技（南京）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、北京惠而特科技有限公司、杭州迪普科技股份有限公司、北京天地和兴科技有限公司、武汉明嘉信信息安全检测评估有限公司、重庆都会信息科技、亚信科技（成都）有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京网御星云信息技术有限公司、泰山信息科技有限公司、星云博创科技有限公司、江西省掌控者信息安全技术有限公司、中国烟草总公司湖北省公司、杭州美创科技有限公司、平安银河实验室、上海纽盾科技股份有限公司、南京树安信息技术有限公司、北京机沃科技有限公司、鹤壁市汇安信息科技有限公司、奇安信-工控安全实验室、广州安亿信软件科技有限公司、东方电气集团科学技术研究院有限公司能源装备工控网络安全工程实验室、武汉绿色网络、北方实验室（沈阳）股份有限公司及其他个人白帽子向 CNVD 提交了 12712 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 10371 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） | 7852 | 7852 |
| 斗象科技（漏洞盒子） | 2015 | 2015 |

| | | |
|---|---|---|
| 北京天融信网络安全技术有限公司 | 608 | 15 |
| 上海交大 | 504 | 504 |
| 哈尔滨安天科技集团股份有限公司 | 273 | 0 |
| 新华三技术有限公司 | 184 | 0 |
| 北京神州绿盟科技有限公司 | 144 | 0 |
| 恒安嘉新(北京)科技股份公司 | 124 | 0 |
| 北京启明星辰信息安全技术有限公司 | 104 | 49 |
| 深信服科技股份有限公司 | 93 | 1 |
| 华为技术有限公司 | 83 | 0 |
| 天津市国瑞数码安全系统股份有限公司 | 81 | 0 |
| 北京数字观星科技有限公司 | 76 | 0 |
| 北京奇虎科技有限公司 | 24 | 0 |
| 南京联成科技发展股份有限公司 | 8 | 8 |
| 杭州安恒信息技术股份有限公司 | 7 | 7 |
| 北京知道创宇信息技术股份有限公司 | 4 | 0 |
| 浙江大华技术股份有限公司 | 3 | 3 |
| 深圳市腾讯计算机系统有限公司（玄武实验室） | 2 | 2 |
| 北京智游网安科技有限公司 | 1 | 1 |

| | | |
|---|---|---|
| 西安四叶草信息技术有限公司 | 1 | 1 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 1 | 1 |
| 山东新潮信息技术有限公司 | 357 | 357 |
| 山东云天安全技术有限公司 | 303 | 303 |
| 联想集团 | 132 | 0 |
| 北京华云安信息技术有限公司 | 87 | 87 |
| 南京众智维信息科技有限公司 | 72 | 72 |
| 中国电信股份有限公司网络安全产品运营中心 | 65 | 64 |
| 北京山石网科信息技术有限公司 | 61 | 61 |
| 浙江木链物联网科技有限公司 | 60 | 60 |
| 河南灵创电子科技有限公司 | 45 | 45 |
| 北京信联科汇科技有限公司 | 36 | 36 |
| 内蒙古洞明科技有限公司 | 34 | 34 |
| 河南信安世纪科技有限公司 | 27 | 27 |
| 广东蓝爵网络安全技术股份有限公司 | 25 | 25 |
| 信联科技（南京）有限公司 | 23 | 23 |
| 内蒙古云科数据服务 | 19 | 19 |

| | | |
|---|---|---|
| 股份有限公司 | | |
| 北京安帝科技有限公司 | 18 | 18 |
| 北京惠而特科技有限公司 | 16 | 16 |
| 杭州迪普科技股份有限公司 | 15 | 0 |
| 北京天地和兴科技有限公司 | 15 | 15 |
| 武汉明嘉信信息安全检测评估有限公司 | 13 | 13 |
| 重庆都会信息科技 | 13 | 13 |
| 亚信科技（成都）有限公司 | 11 | 1 |
| 北京云科安信科技有限公司（Seraph 安全实验室） | 11 | 11 |
| 北京网御星云信息技术有限公司 | 10 | 10 |
| 泰山信息科技有限公司 | 8 | 8 |
| 星云博创科技有限公司 | 6 | 6 |
| 江西省掌控者信息安全技术有限公司 | 6 | 6 |
| 中国烟草总公司湖北省公司 | 4 | 4 |
| 杭州美创科技有限公司 | 3 | 3 |
| 平安银河实验室 | 2 | 2 |
| 上海纽盾科技股份有限公司 | 2 | 2 |
| 南京树安信息技术有限公司 | 2 | 2 |

| | | |
|---|---|---|
| 北京机沃科技有限公司 | 1 | 1 |
| 鹤壁市汇安信息科技有限公司 | 1 | 1 |
| 奇安信-工控安全实验室 | 1 | 1 |
| 广州安亿信软件科技有限公司 | 1 | 1 |
| 东方电气集团科学技术研究院有限公司能源装备工控网络安全工程实验室 | 1 | 1 |
| 武汉绿色网络 | 1 | 1 |
| 北方实验室（沈阳）股份有限公司 | 1 | 1 |
| CNCERT 宁夏分中心 | 7 | 7 |
| CNCERT 贵州分中心 | 3 | 3 |
| CNCERT 青海分中心 | 1 | 1 |
| CNCERT 河北分中心 | 1 | 1 |
| CNCERT 天津分中心 | 1 | 1 |
| 个人 | 894 | 890 |
| 报送总计 | 14607 | 12712 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 550 个漏洞。WEB 应用 216 个，应用程序 145 个，网络设备（交换机、路由器等网络端设备）143 个，操作系统 22 个，智能设备（物联网终端设备）20 个，安全产品 4 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 | 216 |
| 应用程序 | 145 |
| 网络设备（交换机、路由器等网络端设备） | 143 |
| 操作系统 | 22 |
| 智能设备（物联网终端设备） | 20 |
| 安全产品 | 4 |

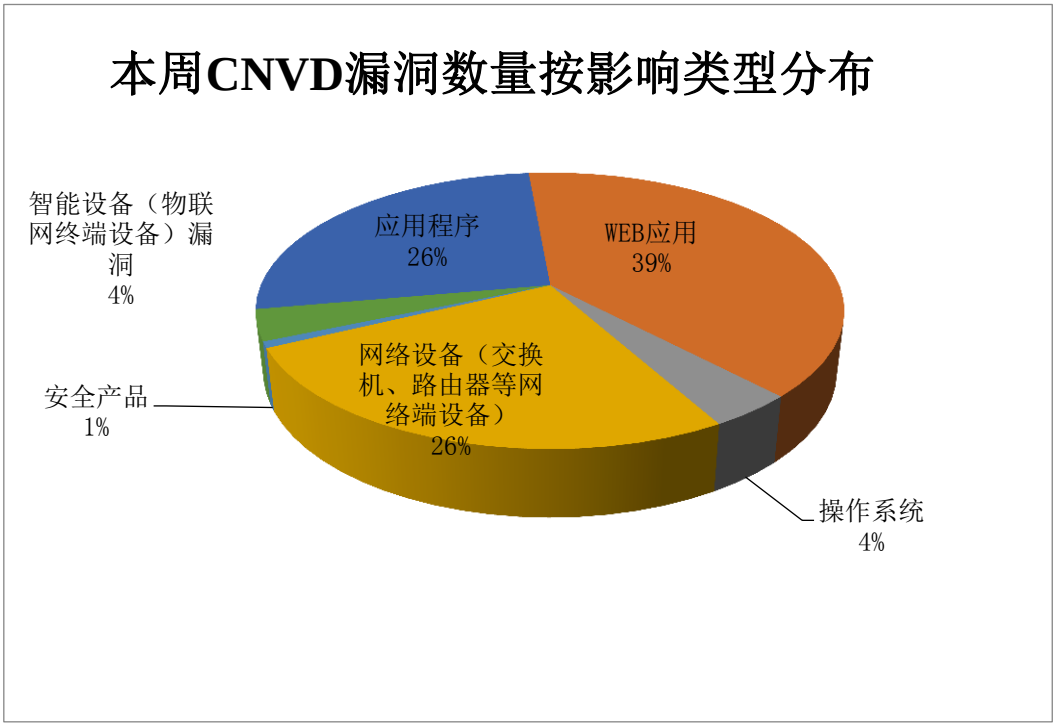


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、NETGEAR、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 | D-Link | 48 | 8% |
| 2 | NETGEAR | 38 | 7% |
| 3 | Google | 29 | 5% |
| 4 | yasm | 18 | 3% |
| 5 | 北京星网锐捷网络技术有限公司 | 15 | 3% |
| 6 | XStream | 14 | 3% |
| 7 | grib-api | 14 | 3% |
| 8 | Microsoft | 12 | 2% |
| 9 | Nitro Software | 10 | 2% |
| 10 | 其他 | 352 | 64% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 111 个电信行业漏洞，29 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-816 命令执行漏洞（CNVD-2021-67516）、Siemens SIMATIC PCS 7 安全绕过漏洞”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/

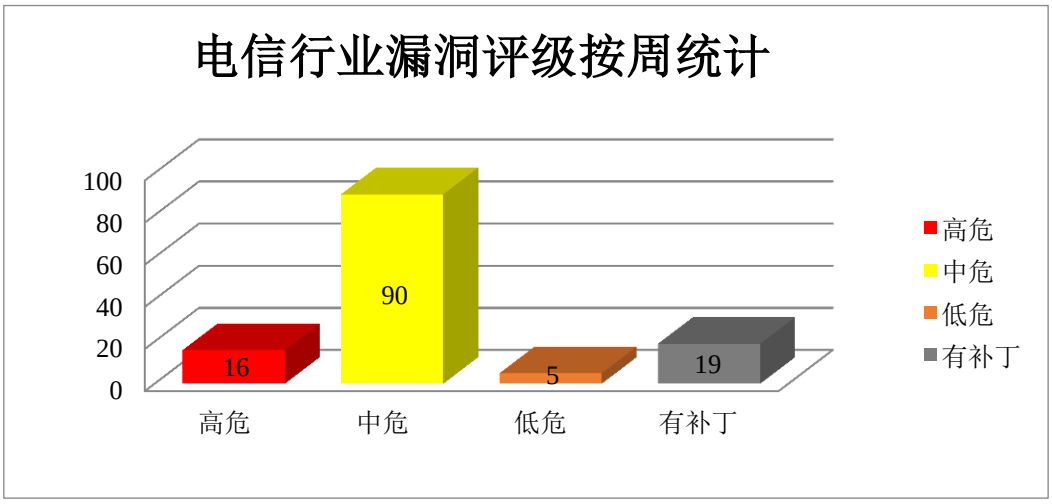


图 3 电信行业漏洞统计

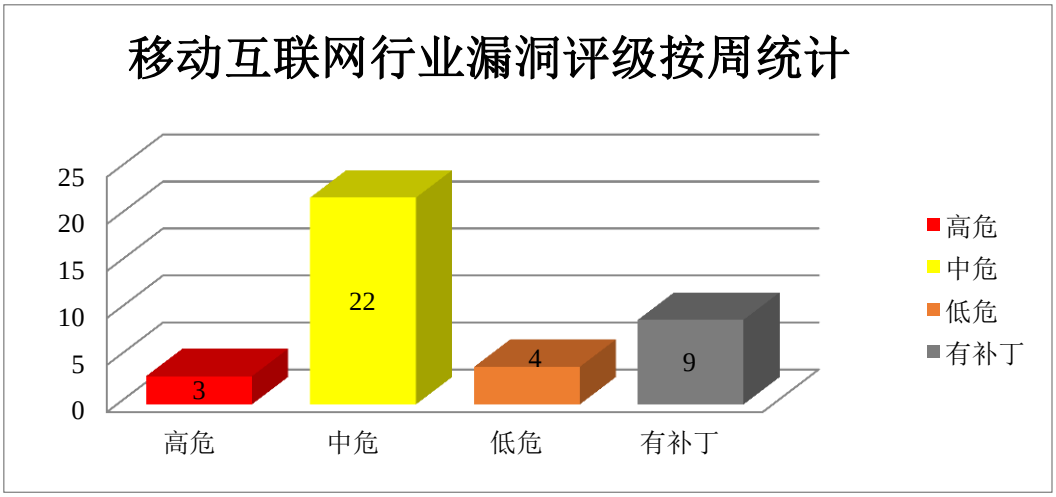


图 4 移动互联网行业漏洞统计

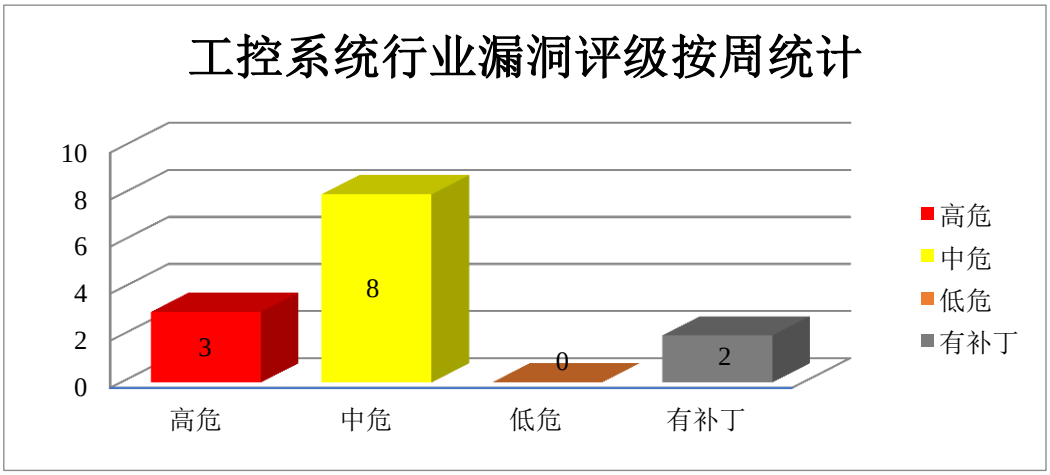

图 5 工控系统行业漏洞统计

## 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、Foxit 产品安全漏洞

Foxit PDF Reader 和 Foxit PDF Editor 都是中国福昕（Foxit）公司的产品。Foxit PDF Reader 是一款 PDF 阅读器。Foxit PDF Editor 是一款 PDF 编辑器。Foxit Phantom PDF 是中国福昕（Foxit）公司的一款 PDF 文档阅读器。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞在处理 XFA 表单或链接对象期间通过递归函数调用堆栈，在将 PDF 文档转换为不同的文档格式期间发生内存损坏，导致 NULL 指针取消引用，或越界读取或写入等。

CNVD 收录的相关漏洞包括：Foxit Reader 和 Foxit PhantomPDF 拒绝服务漏洞、Foxit Reader 和 Foxit PhantomPDF 缓冲区溢出漏洞（CNVD-2021-66414、CNVD-2021-66412）、Foxit PDF Reader 和 Foxit PDF Editor 越界读取漏洞、Foxit PDF Reader 和 Foxit PDF Editor 文件写入漏洞、Foxit PDF Reader 和 Foxit PDF Editor 空指针引用漏洞、Foxit PDF Reader 和 Foxit PDF Editor 拒绝服务漏洞（CNVD-2021-66410、CNVD-2021-66411）。其中“Foxit Reader 和 Foxit PhantomPDF 缓冲区溢出漏洞（CNVD-2021-66414、CNVD-2021-66412）、Foxit PDF Reader 和 Foxit PDF Editor 空指针引用漏洞”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-2021-66413

https://www.cnvd.org.cn/flaw/show/CNVD-2021-66414

https://www.cnvd.org.cn/flaw/show/CNVD-2021-66412

https://www.cnvd.org.cn/flaw/show/CNVD-2021-66408

https://www.cnvd.org.cn/flaw/show/CNVD-2021-66409

https://www.cnvd.org.cn/flaw/show/CNVD-2021-66407

https://www.cnvd.org.cn/flaw/show/CNVD-2021-66410

https://www.cnvd.org.cn/flaw/show/CNVD-2021-66411

### 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。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞在当前用户的上下文中执行任意代码，控制受影响的系统。

CNVD 收录的相关漏洞包括：Microsoft Windows/Windows Server 远程代码执行漏洞（CNVD-2021-67493、CNVD-2021-67492、CNVD-2021-67491、CNVD-2021-67490、

CNVD-2021-67489、CNVD-2021-67488）、Microsoft Windows/Windows Server 权限提升漏洞（CNVD-2021-67495、CNVD-2021-67494）。其中“Microsoft Windows/Windows Server 远程代码执行漏洞（CNVD-2021-67491、CNVD-2021-67490、CNVD-2021-67489、CNVD-2021-67488）”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-2021-67493
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67492
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67491
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67490
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67489
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67488
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67495
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67494

### 3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞使缓冲区溢出，并在系统上执行任意代码，或导致应用程序崩溃，获取敏感信息等。

CNVD 收录的相关漏洞包括：Google Chrome WebRTC 代码执行漏洞（CNVD-2021-67550、CNVD-2021-67551）、Google Chrome WebApp Installs 代码执行漏洞、Google Chrome Web Share 代码执行漏洞、Google Chrome TabStrip 缓冲区溢出漏洞、Google Chrome Sign-In 代码执行漏洞、Google Chrome Permissions 代码执行漏洞、Google Chrome Navigation 信息泄露漏洞（CNVD-2021-67547）。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-2021-67550
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67551
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67540
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67554
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67548
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67553
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67555
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67547

### 4、NETGEAR 产品安全漏洞

NETGEAR M4300-28G 等都是美国网件（NETGEAR）公司的一款网管型交换机。NETGEAR EX7000 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR

R8900 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR R9000 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR D7800 等都是美国网件（NETGEAR）公司的产品。NETGEAR R7500 是一款无线路由器。NETGEAR WNDR 4300 是一款无线路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品权限提升漏洞（CNVD-2021-67654、CNVD-2021-66982、CNVD-2021-66981、CNVD-2021-67655）、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-67658、CNVD-2021-67657、CNVD-2021-67656、CNVD-2021-67653）。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-2021-67654
https://www.cnvd.org.cn/flaw/show/CNVD-2021-66982
https://www.cnvd.org.cn/flaw/show/CNVD-2021-66981
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67655
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67658
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67657
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67656
https://www.cnvd.org.cn/flaw/show/CNVD-2021-67653

### 5、Linux kernel 信息泄露漏洞（CNVD-2021-68182）

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。本周，Linux kernel 被披露存在信息泄露漏洞。攻击者可利用该漏洞读取未初始化的内存。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-2021-68182

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-2021-67513 | ZOHO ManageEngine Log360 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，补丁获取链接：https://www.manageengine.com/log-management/9182736/ManageEngine_Log360_64bit.exe |
| CNVD-2021-67510 | ZOHO ManageEngine Log360 代码问题漏洞 | 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.manageengine.com/log-management/9182736/ManageEngine_Log360_64 |

| | | | |
|---|---|---|---|
| | | | bit.exe |
| CNVD-2021-67504 | WMS SQL 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/FeMiner/wms/issues/7 |
| CNVD-2021-67650 | Rundeck 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://github.com/rundeck/rundeck/security/advisories/GHSA-3jmw-c69h-426c |
| CNVD-2021-66913 | Misskey 跨站脚本漏洞（CNVD-2021-66913） | 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/misskey-dev/misskey/security/advisories/GHSA-pmmv-jwqh-f5ww |
| CNVD-2021-67649 | Mautic 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/mautic/mautic/security/advisories/GHSA-86pv-95mj-7w5f |
| CNVD-2021-67519 | D-Link DSR-500N 默认帐户漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10235 |
| CNVD-2021-67525 | D-Link DSL-2750U OS 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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10230 |
| CNVD-2021-67517 | D-Link DIR-816 命令执行漏洞 | 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.dlink.com/en/security-bulletin/ |
| CNVD-2021-67523 | D-Link DAP-2020 堆栈缓冲区溢出漏洞（CNVD-2021-67523） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新： https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10201 |

小结：本周，Foxit 产品被披露存在多个漏洞，攻击者可利用漏洞在当前登录用户的上下文中执行 JavaScript，在 BIG-IP 系统上造成拒绝服务(DoS)，执行 SSRF 攻击，通过 BIGIP 管理口或 Self IP 地址访问管理页面，来执行任意的系统命令，创建或删除文件，或禁用服务。此外，Microsoft、Google、NETGEAR 等多款产品被披露存在多个漏洞，攻击者可利用漏洞当前用户的上下文中执行任意代码，控制受影响的系统，远程执行命令，从而获得系统权限。另外，Linux kernel 被披露存在信息泄露漏洞。攻击者可利用漏洞读取未初始化的内存。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 Duplicate Page 跨站脚本漏洞

**验证描述**

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

WordPress Duplicate Page 存在跨站脚本漏洞，攻击者可利用漏洞在受影响站点的上下文中执行任意脚本代码，窃取基于 cookie 的身份验证凭据并发起其他攻击。

**验证信息**

POC 链接：https://packetstormsecurity.com/files/164019/WordPress-Duplicate-Page-4.4.1-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-68179

**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. Linphone SIP 堆栈错误可能让攻击者远程使客户端设备崩溃

网络安全研究人员披露了 Linphone 会话启动协议（SIP）堆栈中零点击安全漏洞的详细信息，该漏洞可被远程利用，受害者无需采取任何行动即可使 SIP 客户端崩溃并导致拒绝服务（DoS）条件。

参考链接：https://thehackernews.com/2021/09/linphone-sip-stack-bug-could-let.html

### 2. QNAP 将修补其 NAS 设备中的 OpenSSL 漏洞

NAS 设备制造商 QNAP 正在为其受 OpenSSL 漏洞（现已修复）影响的产品开发安全补丁。

参考链接：https://securityaffairs.co/wordpress/121724/iot/qnap-openssl-nas.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