国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 06 月 21 日-2021 年 06 月 27 日　　2021 年第 25 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 605 个，其中高危漏洞 168 个、中危漏洞 363 个、低危漏洞 74 个。漏洞平均分值为 5.59。本周收录的漏洞中，涉及 0day 漏洞 327 个（占 54%），其中互联网上出现“Liftoff GateOne 任意命令执行漏洞、White Shark System（WSS）跨站请求伪造漏洞”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 3577 个，与上周（2579 个）环比增加 39%。

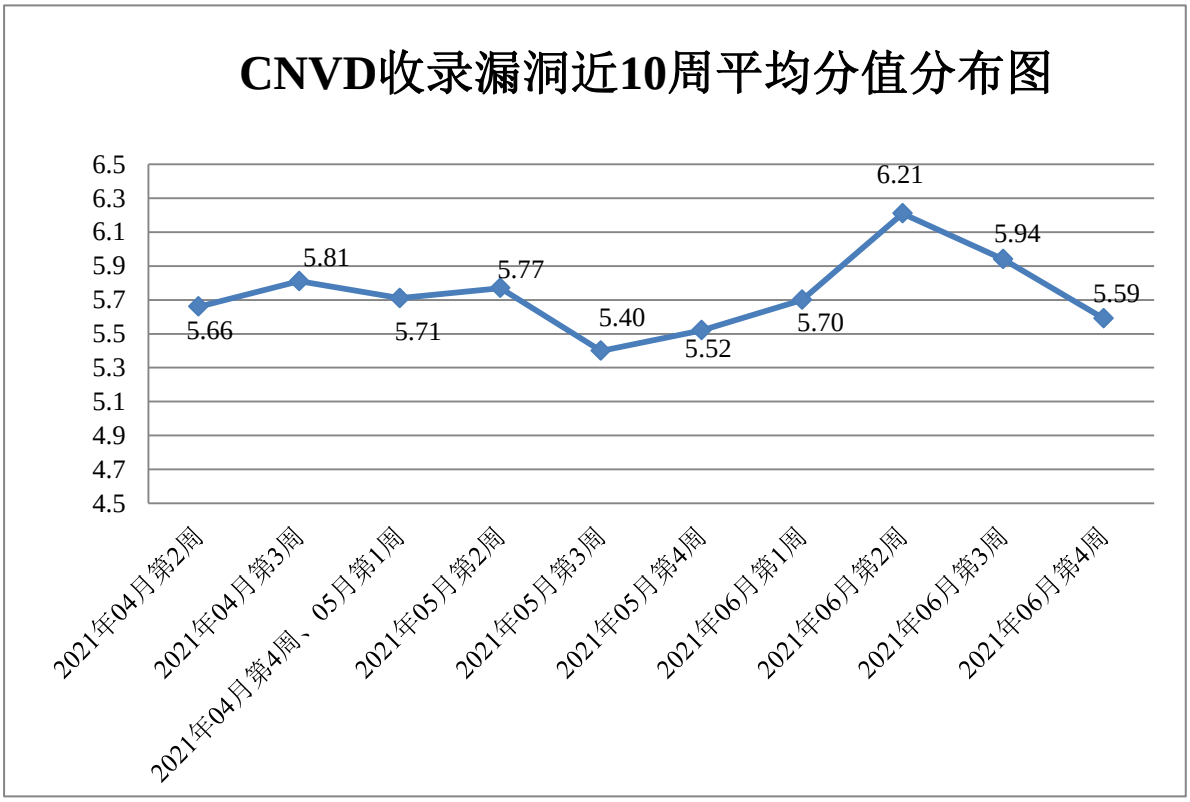

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 41 起，向基础电信企业通报漏洞事件 25 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 369 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 42 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 31 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、重庆泛普科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、长沙市同迅计算机科技有限公司、长沙德尚网络科技有限公司、新都（青岛）办公系统有限公司、新道科技股份有限公司、襄阳市番茄网络科技有限公司、夏普商贸（中国）有限公司、西安紫云羚网络科技有限责任公司、西安新软信息科技有限公司、西安大西信息科技有限公司、武汉烽火信息集成技术有限公司、潍坊家园驿站电子技术有限公司、同方股份有限公司、天信仪表集团有限公司、腾亿网络科技有限公司、松下电器（中国）有限公司、四创科技有限公司、四川迅睿云软件开发有限公司、四川聚美恒星网络科技有限公司、思科系统（中国）网络技术有限公司、施耐德电气（中国）有限公司、深圳市中科网威科技有限公司、深圳市正业玖坤信息技术有限公司、深圳市区域网络科技服务有限公司、深圳市乔安科技有限公司、深圳市美科星通信技术有限公司、深圳市领空技术有限公司、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、深圳市红果软件有限公司、深圳市果谷网络有限公司、深圳市朝恒辉科技有限公司、深圳汉光电子技术有限公司、上海亦存网络科技有限公司、上海图鸭信息科技有限公司、上海米健信息技术有限公司、上海蓝山办公软件有限公司、上海华测导航技术股份有限公司、上海博达数据通信有限公司、上海安达通信息安全技术股份有限公司、熵基科技股份有限公司、厦门市灵鹿谷科技有限公司、厦门海为科技有限公司、三星（中国）投资有限公司、任子行网络技术股份有限公司、青岛灼灼文化传媒有限公司、青岛万物一体网络科技有限公司、纽仁信息科技（上海）有限公司、朗坤智慧科技股份有限公司、蓝盾信息安全技术股份有限公司、科大讯飞股份有限公司、柯尼卡美能达（中国）投资有限公司、金蝶软件（中国）有限公司、济南爱程网络科技有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、湖南考试在线网络科技有限公司、湖北点点点科技有限公司、杭州新中大科技股份有限公司、杭州海康威视数字技术股份有限公司、杭州二维火科技有限公司、杭州安恒信息技术股份有限公司、国泰新点软件股份有限公司、广州众米信息科技有限公司、广州唯众网络科技有限公司、广联达科技股份有限公司、谷歌公司、富士施乐（中国）有限公司、戴尔（中国）有限公司、大唐电信科技股份有限公司、大连华天软件有限公

司、成都索贝数码科技股份有限公司、成都爱米秀科技有限责任公司、北京中远麒麟科技有限公司、北京中创视讯科技有限公司、北京致远互联软件股份有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京小度互娱科技有限公司、北京伟联科技有限公司、北京天融信网络安全技术有限公司、北京神州数码云科信息技术有限公司、北京灵州网络技术有限公司、北京兰德华电子技术有限公司、北京金风易通科技有限公司、北京博昊天成科技有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、爱思华宝中国公司、爱普生（中国）有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、联想集团、京东云安全、成都零起飞网络、千旺软件、阿里巴巴集团安全应急响应中心、百度安全应急响应中心、快排 CMS、万通 CMS、贴心猫（imcat）、YApi、TPCMS、The Apache Software Foundation、Textpattern CMS、SEACMS、PowerJob、PCFCMS、PACOM Systems Pty Ltd、NETGEAR、MuYuCMS、Multilaser、MOBOTIX、Lexmark、Kyan、Kong Inc.、Joomla!、bluecms、beecms 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、北京神州绿盟科技有限公司、恒安嘉新（北京）科技股份公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。广州易东信息安全技术有限公司、北京信联科汇科技有限公司、北京山石网科信息技术有限公司、河南信安世纪科技有限公司、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、武汉明嘉信信息安全检测评估有限公司、长春嘉诚信息技术股份有限公司、山东泽鹿安全技术有限公司、北京天地和兴科技有限公司、北京安帝科技有限公司、北京华云安信息技术有限公司、山东云天安全技术有限公司、江西省掌控者信息安全技术有限公司、北京蓝森科技有限公司、重庆贝特计算机系统工程有限公司、安徽长泰信息安全服务有限公司、百度在线网络技术有限公司、杭州天谷信息科技有限公司、杭州木链物联网科技有限公司、北方实验室（沈阳）股份有限公司、浙江御安信息技术有限公司、星云博创科技有限公司、任子行网络技术股份有限公司、北京机沃科技有限公司、北京顶象技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、重庆都会信息科技有限公司、广州安亿信软件科技有限公司、广州万蓝宝田科技发展有限公司、日照天鳌网络科技有限公司、深圳市魔方安全科技有限公司、亚信科技（成都）有限公司、中国工程物理研究院计算机应用研究所、中国工商银行、中移（杭州）信息技术有限公司、中资网络信息安全科技有限公司及其他个人白帽子向 CNVD 提交了 3577 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 1688 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）	1007	1007
上海交大	343	343
奇安信网神（补天平台）	338	338
北京天融信网络安全技术有限公司	309	9
哈尔滨安天科技集团股份有限公司	215	0
北京神州绿盟科技有限公司	148	6
恒安嘉新（北京）科技股份公司	125	0
北京数字观星科技有限公司	120	0
深信服科技股份有限公司	108	1
华为技术有限公司	94	0
远江盛邦（北京）网络安全科技股份有限公司	77	77
卫士通信息产业股份有限公司	50	0
北京启明星辰信息安全技术有限公司	50	0
天津市国瑞数码安全系统股份有限公司	49	0
西安四叶草信息技术有限公司	21	21
北京知道创宇信息技术股份有限公司	4	0
北京长亭科技有限公司	1	1
杭州安恒信息技术股	1	1

份有限公司		
广州易东信息安全技术有限公司	309	309
北京信联科汇科技有限公司	129	129
北京山石网科信息技术有限公司	82	82
河南信安世纪科技有限公司	43	43
河南灵创电子科技有限公司	41	41
南京众智维信息科技有限公司	28	28
武汉明嘉信信息安全检测评估有限公司	25	25
长春嘉诚信息技术股份有限公司	25	25
中国电信股份有限公司网络安全产品运营中心	20	0
山东泽鹿安全技术有限公司	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	13	13
北京安帝科技有限公司	11	11
北京华云安信息技术有限公司	11	11
山东云天安全技术有限公司	11	11
江西省掌控者信息安全技术有限公司	11	11

北京蓝森科技有限公司	9	9
重庆贝特计算机系统工程有限公司	9	9
安徽长泰信息安全服务有限公司	8	8
百度在线网络技术有限公司	8	8
杭州天谷信息科技有限公司	8	8
杭州木链物联网科技有限公司	7	7
北方实验室（沈阳）股份有限公司	6	6
浙江御安信息技术有限公司	5	5
星云博创科技有限公司	3	3
任子行网络技术股份有限公司	2	2
北京机沃科技有限公司	2	2
北京顶象技术有限公司	2	2
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
重庆都会信息科技有限公司	2	2
广州安亿信软件科技有限公司	1	1
广州万蓝宝田科技发展有限公司	1	1
日照天鋆网络科技有限公司	1	1

深圳市魔方安全科技有限公司	1	1
亚信科技（成都）有限公司	1	1
中国工程物理研究院计算机应用研究所	1	1
中国工商银行	1	1
中移（杭州）信息技术有限公司	1	1
中资网络信息安全科技有限公司	1	1
CNCERT 宁夏分中心	41	41
CNCERT 吉林分中心	13	13
CNCERT 辽宁分中心	5	5
CNCERT 广西分中心	4	4
CNCERT 河北分中心	4	4
CNCERT 西藏分中心	4	4
CNCERT 青海分中心	2	2
CNCERT 甘肃分中心	1	1
个人	862	862
报送总计	4868	3577

本周漏洞按类型和厂商统计

本周，CNVD 收录了 605 个漏洞。应用程序 186 个，WEB 应用 164 个，操作系统 86 个，网络设备（交换机、路由器等网络端设备）62 个，智能设备（物联网终端设备）61 个，安全产品 45 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	186
WEB 应用	164
操作系统	86
网络设备（交换机、路由器等网络端设备）	62
智能设备（物联网终端设备）	61
安全产品	45
数据库	1

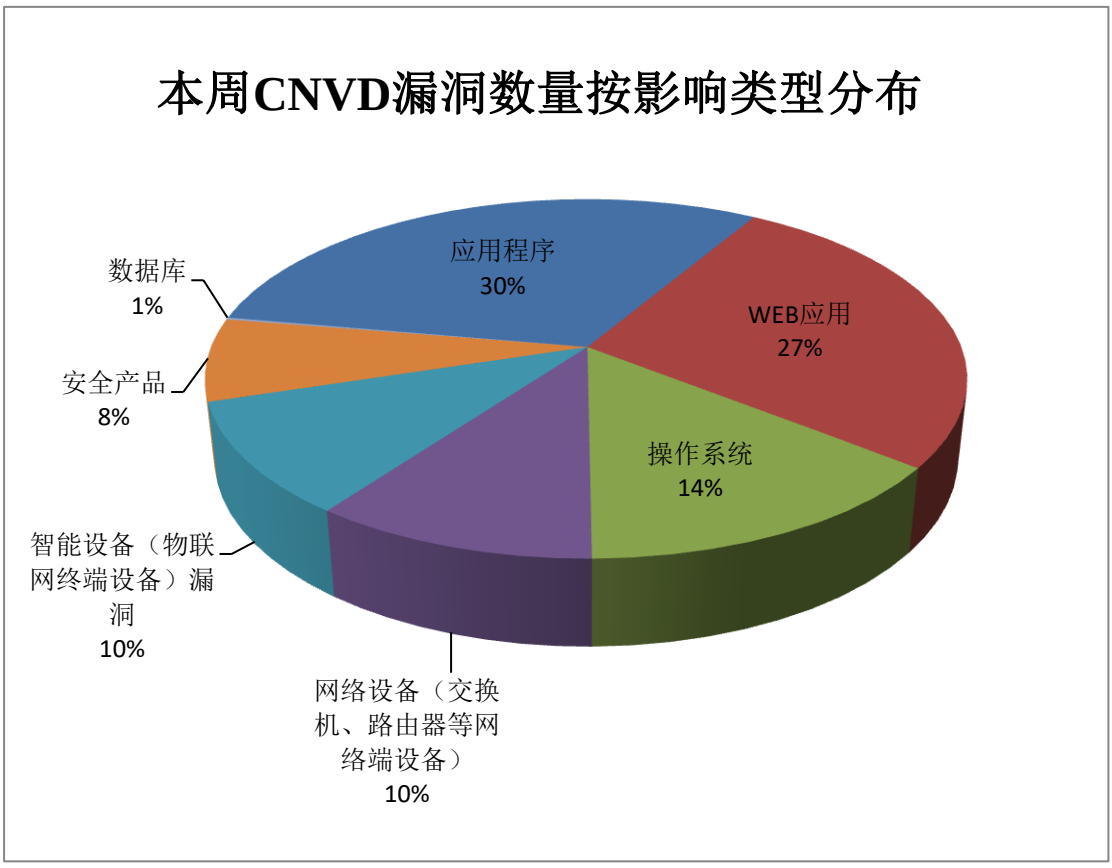

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、WordPress、NETGEAR 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	65	11%
2	WordPress	25	4%
3	NETGEAR	19	3%
4	Axis Communications AB	17	3%
5	Cisco	16	3%
6	松下电器（中国）有限公司	15	2%
7	《中国学术期刊（光盘版）》电子杂志社有限公司	11	2%
8	Samsung	10	2%
9	White Shark System	9	1%
10	其他	418	69%

本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，76 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“TOTOLINK T10 路由器存在命令执行漏洞（CNVD-2021-44931）、Google Android p2p_pd.c 权限提升漏洞、Facebook Hermes 输入验证错误漏洞、D-Link DIR-2640-US 账户密码明文存储漏洞”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/

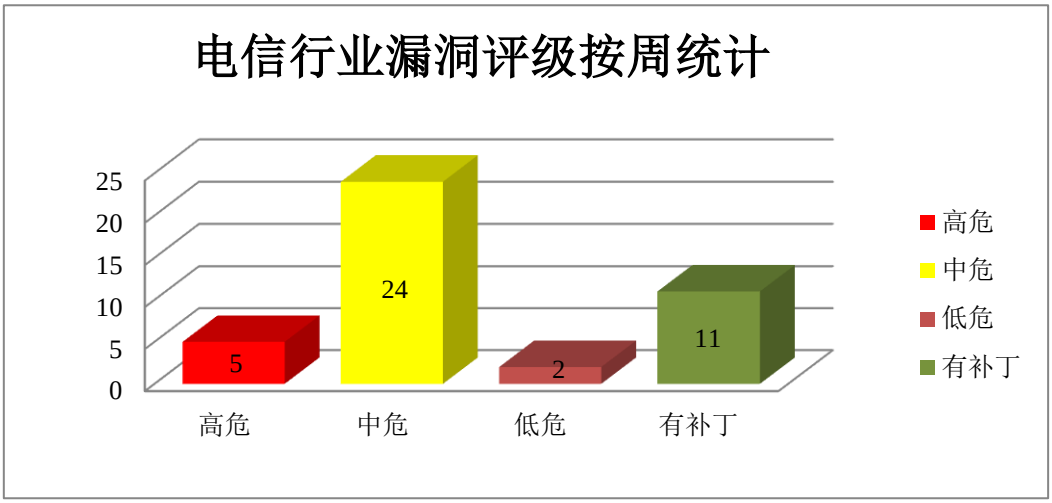

图 3 电信行业漏洞统计

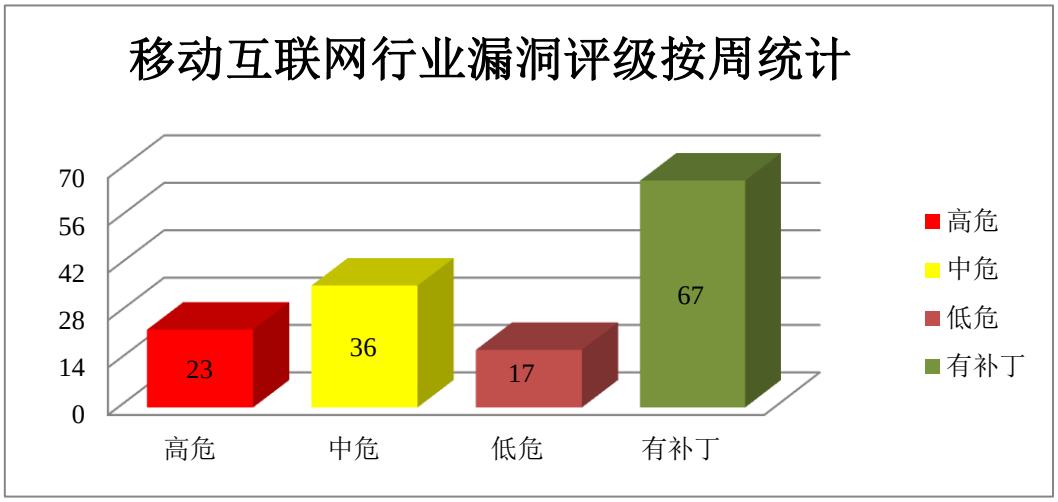

图 4 移动互联网行业漏洞统计

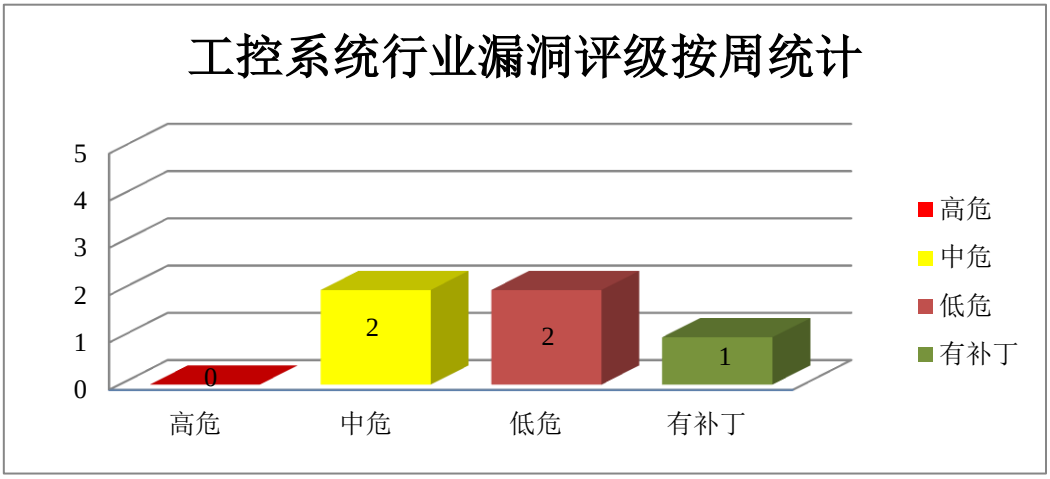

图 5 工控系统行业漏洞统计

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、 WordPress 产品安全漏洞

WordPress 是 Wordpress 基金会的一套使用 PHP 语言开发的博客平台。WP-CLI 是 WordPress 的命令行界面。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞拦截通信，获取管理员 cookie，远程执行代码。

CNVD 收录的相关漏洞包括：WordPress 插件跨站脚本漏洞（CNVD-2021-44297）、WordPress 跨站脚本漏洞（CNVD-2021-44302、CNVD-2021-44303、CNVD-2021-44304、CNVD-2021-44307、CNVD-2021-44309）、WordPress 代码问题漏洞（CNVD-2021-44308）、WordPress WP-CLI 信任管理问题漏洞。其中，“WordPress 代码问题漏洞（CNVD-2021-44308）、WordPress WP-CLI 信任管理问题漏洞”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-2021-44297

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44302

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44303

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44304

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44308

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44307

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44309

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44970

2、Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的的一套以 Linux 为基础的开源操作系

统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Google Android 内存管理驱动程序权限提升漏洞（CNVD-2021-44313、CNVD-2021-44312、CNVD-2021-44311、CNVD-2021-44316、CNVD-2021-44315、CNVD-2021-44314）、Google Android System 权限绕过漏洞（CNVD-2021-44320）、Google Android System 远程代码执行漏洞（CNVD-2021-44329）。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-2021-44313
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44312
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44311
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44316
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44315
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44314
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44320
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44329

3、Cisco 产品安全漏洞

Cisco Firepower Threat Defense 和 Cisco Adaptive Security Appliance 都是美国思科（Cisco）公司的产品。Cisco Firepower Threat Defense 是一套提供下一代防火墙服务的统一软件。Cisco Adaptive Security Appliance 是一套防火墙和网络安全平台。该平台提供了对数据和网络资源的高度安全的访问等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞打破信任链并将代码注入设备的启动过程，在界面上下文中执行任意脚本代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：Cisco Adaptive Security Appliance 和 Cisco Firepower Threat Defense 跨站脚本漏洞（CNVD-2021-44675）、Cisco Adaptive Security Appliance 和 Firepower Threat Defense 安全启动绕过漏洞、Cisco Adaptive Security Appliance 和 Cisco Firepower Threat Defense 拒绝服务漏洞（CNVD-2021-44680、CNVD-2021-44678、CNVD-2021-44684、CNVD-2021-44682）、Cisco Adaptive Security Appliance 和 Cisco Firepower Threat Defense 内存泄露漏洞、Cisco Adaptive Security Appliance 跨站脚本漏洞（CNVD-2021-44674）。其中，“Cisco Adaptive Security Appliance 和 Cisco Firepower Threat Defense 拒绝服务漏洞（CNVD-2021-44678、CNVD-2021-44684、CNVD-2021-44682）、Cisco Adaptive Security Appliance 和 Cisco Firepower Threat Defense 内存泄露漏洞”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-2021-44675
https://www.cnvd.org.cn/flaw/show/CNVD-2021-44674

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44681

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44680

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44678

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44684

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44683

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44682

4、NETGEAR 产品安全漏洞

NETGEAR RBK752 等都是美国网件（NETGEAR）公司的一套家庭 WiFi 系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意 Shell 命令。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品操作系统命令注入漏洞（CNVD-2021-44783、CNVD-2021-44782、CNVD-2021-44786、CNVD-2021-44785、CNVD-2021-44784、CNVD-2021-44787）、多款 NETGEAR 产品命令注入漏洞（CNVD-2021-44781、CNVD-2021-44780）。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-2021-44783

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44782

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44781

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44780

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44786

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44785

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44784

https://www.cnvd.org.cn/flaw/show/CNVD-2021-44787

5、TrendNet TW100-S4W1CA 跨站脚本漏洞

TrendNet TW100-S4W1CA 是一款四端口宽带路由器。本周，TrendNet TW100-S4W1CA 2.3.32 版被披露存在跨站脚本漏洞。攻击者可通过 echo 命令利用该漏洞将任意 JavaScript 注入路由器的 Web 界面。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-2021-45305

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-2021-43997	深信服防火墙管理系统 AF 和上网行为管理系统 AC 存在命令执行漏洞	高	厂商已发布相关漏洞补丁链接，详情关注深信服产品安全中心：https://www.sangfor.com.cn/

CNVD-2021-44268	Contiki-NG 缓冲区溢出漏洞（CNVD-2021-44268）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-6xf2-77gf-fgjx
CNVD-2021-44274	SerenityOS 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://github.com/SerenityOS/serenity/pull/5713/commits/3844e8569689dd476064a0759d704bc64fb3ca2c
CNVD-2021-44929	TOTOLINK T10 路由器存在命令执行漏洞（CNVD-2021-44929）	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：http://www.totolink.cn/
CNVD-2021-44945	D-Link AC2600 权限提升漏洞	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-jabber-GuC5mLwG
CNVD-2021-44956	SonicWall NSM On-Prem 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://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0014
CNVD-2021-44965	Vmware vSphere Client 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://www.vmware.com/security/advisories/VMSA-2021-0010.html
CNVD-2021-44977	IPFire Firewall 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://github.com/ipfire/ipfire-2.x/commit/6769d909306d7bdc43d64598872126fcf1b217f6
CNVD-2021-45279	Microsoft SharePoint 远程代码执行漏洞（CNVD-2021-45279）	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-2020-17118
CNVD-2021-45286	phpMyAdmin SQL 注入漏洞（CNVD-2021-45286）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.phpmyadmin.net/security/PMASA-2020-6/

小结：本周，WordPress 产品被披露存在多个漏洞，攻击者可利用漏洞拦截通信，获取管理员 cookie，远程执行代码。此外，Google、Cisco、NETGEAR 等多款产品被披露存在多个漏洞，攻击者可利用漏洞打破信任链并将代码注入设备的启动过程，提升权限，执行任意代码，导致拒绝服务等。另外，TrendNet TW100-S4W1CA 2.3.32 版被披露

存在跨站脚本漏洞。攻击者可通过 echo 命令利用该漏洞将任意 JavaScript 注入路由器的 Web 界面。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、Liftoff GateOne 任意命令执行漏洞

验证描述

Liftoff GateOne 是一个基于 HTML5 实现的终端模拟器和 SSH 客户端。

Liftoff GateOne 存在任意命令执行漏洞。远程攻击者可在尝试建立 SSH 连接时通过端口字段中的 shell 元字符利用该漏洞执行任意命令。

验证信息

POC 链接：https://github.com/liftoff/GateOne/issues/736

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-45278

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. 戴尔又现高危漏洞，近 3000 万台电脑面临被远程控制风险

据 Eclypsium 网络安全研究人员 6 月 24 日披露，戴尔客户端 BIOS 内的 BIOSConnect 功能存在 4 个严重漏洞。这些漏洞会影响 129 款型号近 3000 万台戴尔电脑，攻击者可以借此远程执行任意代码（RCE）、颠覆操作系统、破坏设备。

参考链接：https://www.freebuf.com/news/278644.html

2. Linux Pling Store 应用程序中未修补的漏洞可能导致供应链攻击

网络安全研究人员披露了一个影响 Linux 平台基于 Pling 的免费和开源软件(FOSS)市场的未修补的关键漏洞，该漏洞可能被滥用以进行供应链攻击并实现远程代码执行（RCE）。

参考链接：https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.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