国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 05 月 30 日-2022 年 06 月 05 日 **2022 年第 22 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 589 个，其中高危漏洞 219 个、中危漏洞 322 个、低危漏洞 48 个。漏洞平均分值为 6.04。本周收录的漏洞中，涉及 0day 漏洞 497 个（占 84%），其中互联网上出现“Tenda AC9 缓冲区溢出漏洞、D-Link DIR-816 A2 命令注入漏洞”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事件型漏洞总数 4943 个，与上周（11141 个）环比减少 56%。

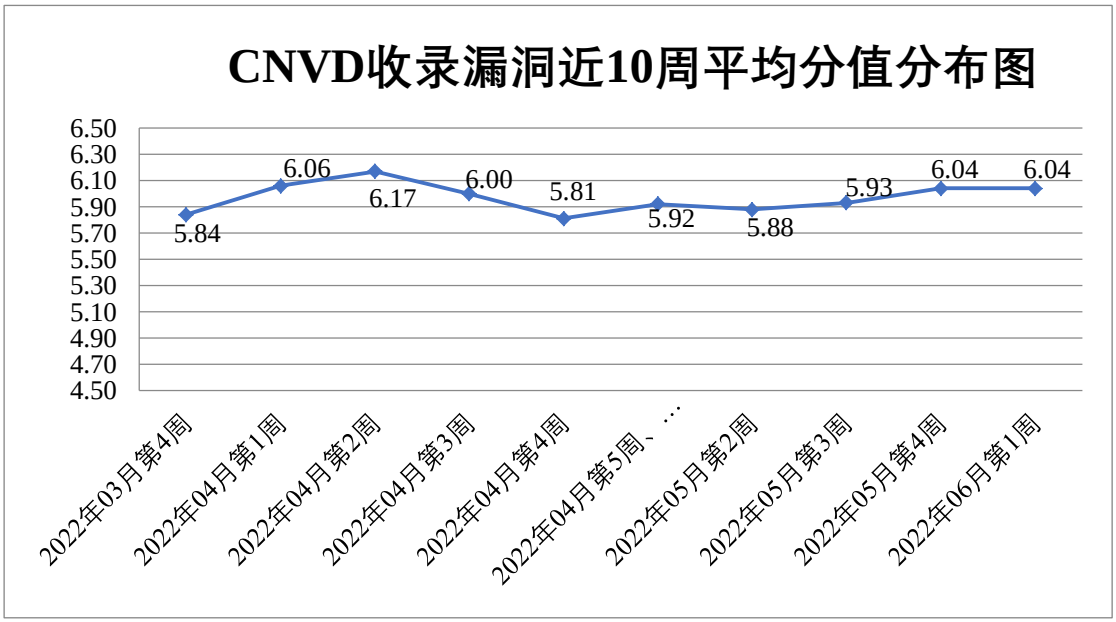

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 26 起，向基础电信企业通报漏洞事件 33 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 813 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 132 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 113 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：

中电光谷建筑设计院有限公司、正方软件股份有限公司、浙江中控技术股份有限公司、浙江慕枫网络科技有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、小白智能科技（长春）股份有限公司、武汉微问网络科技有限公司、台达电子企业管理（上海）有限公司、深圳智慧光迅信息技术有限公司、深圳市迅捷通信技术有限公司、深圳市同享软件科技有限公司、深圳市联软科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市大疆创新科技有限公司、深圳市丛文科技有限公司、深圳市艾珂云谷信息技术有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、熵基科技股份有限公司、山西企凝信息科技有限公司、山东金钟科技集团股份有限公司、厦门四信物联网科技有限公司、锐捷网络股份有限公司、麒麟软件有限公司、普联技术有限公司、明博教育科技股份有限公司、绿盟科技集团股份有限公司、联奕科技股份有限公司、廊坊市极致网络科技有限公司、昆明云涛科技有限公司、金蝶软件（中国）有限公司、江西金磊科技发展有限公司、江苏金智教育信息股份有限公司、吉翁电子（深圳）有限公司、华磊信息科技有限公司、恒锋信息科技股份有限公司、杭州拓康自动化设备有限公司、杭州海康威视数字技术股份有限公司、杭州晨科软件技术有限公司、海南赞赞网络科技有限公司、海海海计算机软件有限公司、哈尔滨伟成科技有限公司、桂林崇胜网络科技有限公司、广州市卓创教育信息科技有限公司、广州市粤海网络科技有限公司、广州市凝智科技有限公司、广联达科技股份有限公司、富士施乐（中国）有限公司、方正科技集团股份有限公司、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、北京五指互联科技有限公司、北京网康科技有限公司、北京天生创想信息技术有限公司、北京硕人时代科技股份有限公司、北京火绒网络科技有限公司、北京东方通科技股份有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、网新科技、三菱电机株式会社、若依、信呼、ZCOMAX TECHNOLOGIES, INC、YZNCMS、The Apache Software Foundation、taocms、SEMCMS、NETGEAR、MuYuCMS、MOBOTIX、Google、FTCMS、Eclipse、CSZCMS、bandisoft 和 Adobe。

本周，CNVD 发布了《关于微软支持诊断工具 MSDT 存在远程代码执行漏洞的安全公告》、《关于 Confluence 存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7746

https://www.cnvd.org.cn/webinfo/show/7756

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、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。武汉安域信息安全技术有限公司、北京山石网科信息技术有限公司、重庆都会信息科技有限公司、北京网御星云信息技术有限公司、上海纽盾科技股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、巨鹏信息科技有限公司、河南信安世纪科技有限公司、广州百蕴启辰科技有限公司、贵州泰若数字科技有限公司、北京升鑫网络科技有限公司、北京远禾科技有限公司、上海观安信息技术股份有限公司、海通证券股份有限公司、中国烟草总公司湖北省公司、山东云天安全技术有限公司、北方实验室（沈阳）股份有限公司、四川赛闯检测股份有限公司及其他个人白帽子向 CNVD 提交了 4943 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 2791 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）	2086	2086
奇安信网神（补天平台）	559	559
上海交大	146	146
阿里云计算有限公司	712	0
杭州安恒信息技术股份有限公司	482	213
深信服科技股份有限公司	174	0
安天科技集团股份有限公司	171	0
新华三技术有限公司	162	0
北京数字观星科技有限公司	154	0
北京天融信网络安全技术有限公司	132	2
恒安嘉新（北京）科技股份公司	101	0

天津市国瑞数码安全系统股份有限公司	59	0
北京启明星辰信息安全技术有限公司	56	0
京东科技信息技术有限公司	32	20
西安四叶草信息技术有限公司	32	32
北京长亭科技有限公司	15	15
内蒙古云科数据服务股份有限公司	14	14
中国电信集团系统集成有限责任公司	12	0
远江盛邦（北京）网络安全科技股份有限公司	2	2
北京知道创宇信息技术股份有限公司	2	0
南京联成科技发展股份有限公司	1	1
南京众智维信息科技有限公司	1	1
北京华顺信安科技有限公司	185	0
武汉安域信息安全技术有限公司	22	22
北京山石网科信息技术有限公司	21	21
重庆都会信息科技有限公司	19	19
北京网御星云信息技术有限公司	19	19
上海纽盾科技股份有限公司	14	14

杭州迪普科技股份有限公司	12	0
北京云科安信科技有限公司（Seraph 安全实验室）	7	7
巨鹏信息科技有限公司	5	5
河南信安世纪科技有限公司	4	4
广州百蕴启辰科技有限公司	3	3
贵州泰若数字科技有限公司	3	3
北京升鑫网络科技有限公司	2	2
北京远禾科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
海通证券股份有限公司	1	1
中国烟草总公司湖北省公司	1	1
山东云天安全技术有限公司	1	1
北方实验室（沈阳）股份有限公司	1	1
四川赛闯检测股份有限公司	1	1
CNCERT 浙江分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 山西分中心	1	1
CNCERT 四川分中心	1	1
个人	1722	1722

报送总计	7154	4943

本周漏洞按类型和厂商统计

本周，CNVD 收录了 589 个漏洞。WEB 应用 311 个，应用程序 112 个，网络设备（交换机、路由器等网络端设备）86 个，智能设备（物联网终端设备）39 个，操作系统 28 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
WEB 应用	311
应用程序	112
网络设备（交换机、路由器等网络端设备）	86
智能设备（物联网终端设备）	39
操作系统	28
安全产品	10
数据库	3

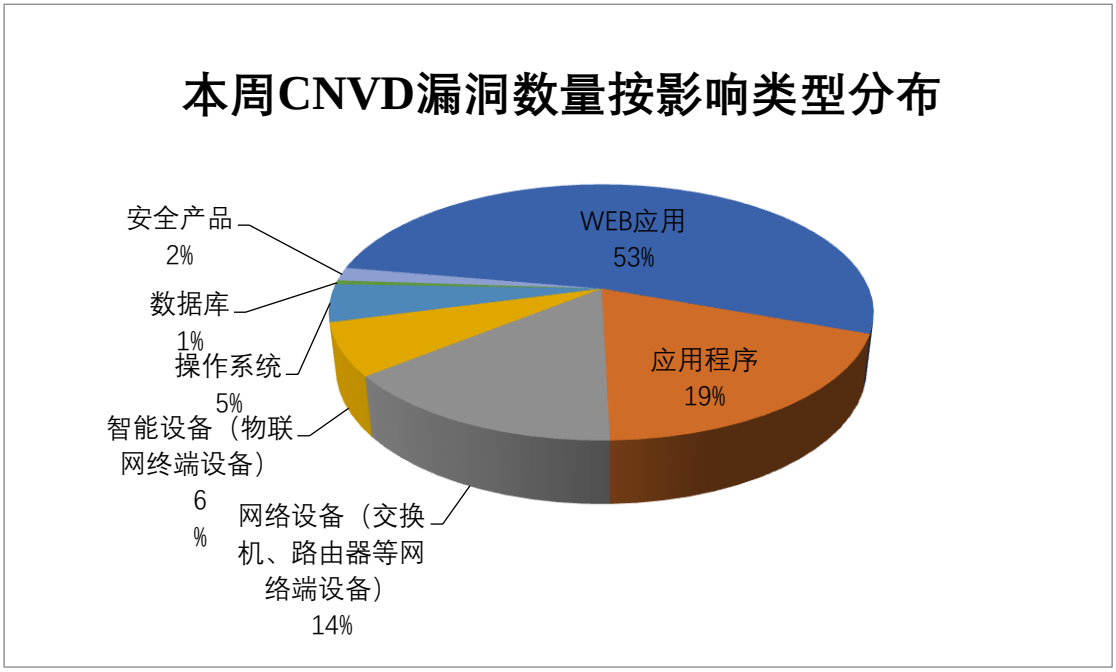

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Google、Adobe 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	24	4%

2	Google	19	3%
3	Adobe	18	3%
4	Tenda	12	2%
5	D-Link	12	2%
6	Dell	11	2%
7	Brother	8	1%
8	兄弟（中国）商业有限公司	7	1%
9	TOTOLINK	7	1%
10	其他	471	81%

本周行业漏洞收录情况

本周，CNVD 收录了 69 个电信行业漏洞，49 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 A3100R 缓冲区溢出漏洞、Tenda AX12 缓冲区溢出漏洞（CNVD-2022-42152）”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/

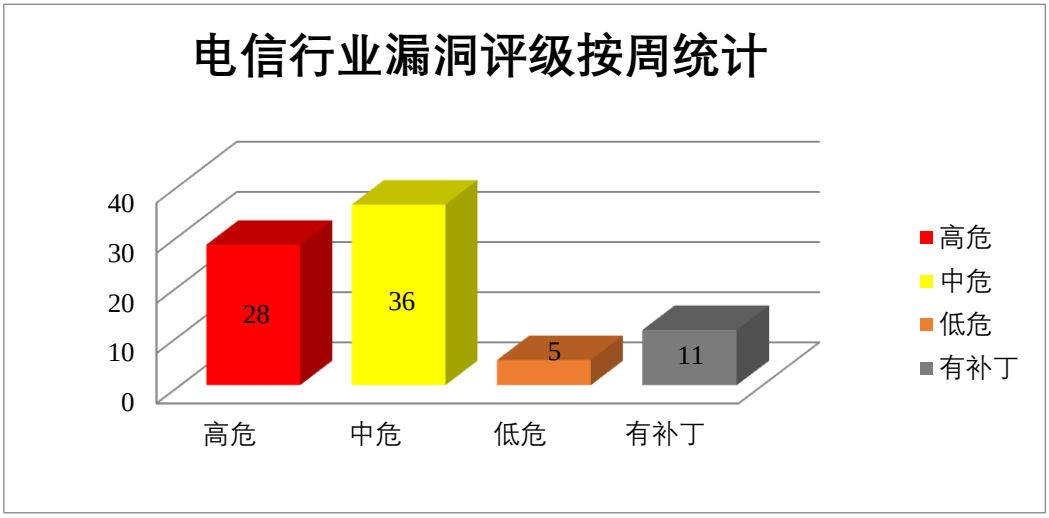

图 3 电信行业漏洞统计

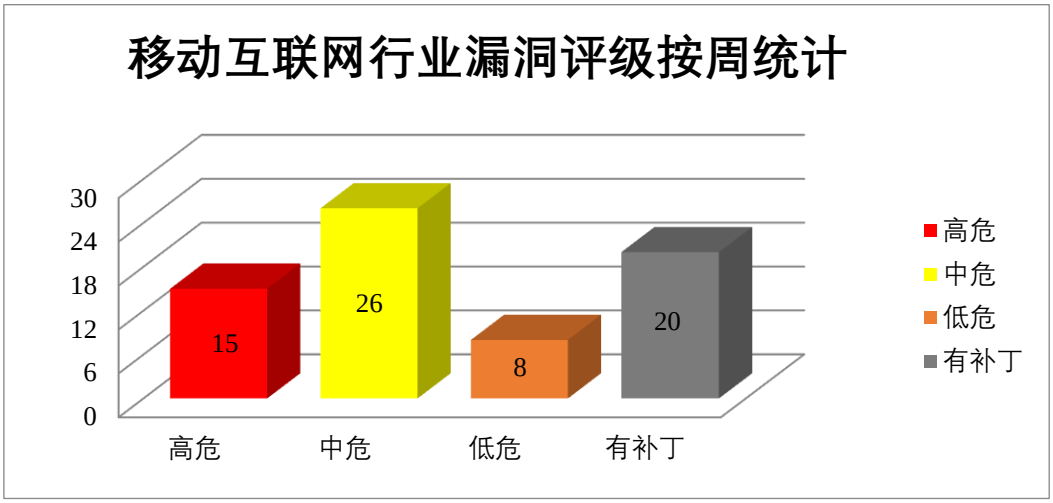

图 4 移动互联网行业漏洞统计

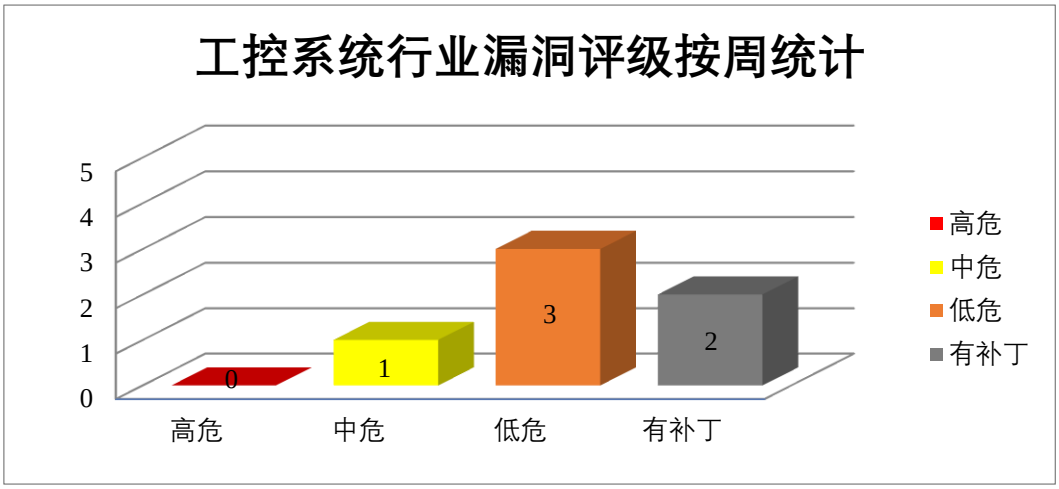

图 5 工控系统行业漏洞统计

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 Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Photoshop 输入验证错误漏洞、Adobe Photoshop 越界写入漏洞（CNVD-2022-42165、CNVD-2022-42164、CNVD-2022-42169、CNVD-2022-42168、CNVD-2022-42167、CNVD-2022-42171、CNVD-2022-42170）。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-2022-42166

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42165

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42164

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42169

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42168

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42167

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42171

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42170

2、 Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的一套以 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。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-42138、CNVD-2022-42142、CNVD-2022-42141、CNVD-2022-42140、CNVD-2022-42139、CNVD-2022-42143、CNVD-2022-42148、CNVD-2022-42147）。其中，除“Google Android 权限提升漏洞（CNVD-2022-42148）、Google Android 权限提升漏洞（CNVD-2022-42147）”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-2022-42138

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42142

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42141

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42140

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42139

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42143

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42148

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42147

3、 WordPress 产品安全漏洞

WordPress 是一套使用 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。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 SQL 注入攻击，删除缓存，删除源，创建源，上传恶意文件从而远程执行任意代码等。

CNVD 收录的相关漏洞包括：WordPress Hermit plugin SQL 注入漏洞、WordPress Hermit plugin 跨站请求伪造漏洞、WordPress VikBooking Hotel Booking Engine&PMS plugin 信息泄露漏洞、WordPress VikBooking Hotel Booking Engine&PMS plugin 任意文件上传漏洞、WordPress Booking Calendar plugin 代码问题漏洞、WordPress Daily Prayer Time plugin SQL 注入漏洞、WordPress 插件 Donations SQL 注入漏洞、WordPress 插件 Users Ultra SQL 注入漏洞。其中，除“WordPress Hermit plugin 跨站请求伪造漏洞、WordPress VikBooking Hotel Booking Engine&PMS plugin 信息泄露漏洞、WordPress Booking Calendar plugin 代码问题漏洞”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-2022-41790

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41791

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41801

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41800

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41799

https://www.cnvd.org.cn/flaw/show/CNVD-2022-41807

https://www.cnvd.org.cn/flaw/show/CNVD-2022-43220

https://www.cnvd.org.cn/flaw/show/CNVD-2022-43221

4、Dell 产品安全漏洞

Dell Vnx2Oe For File 是美国戴尔（Dell）公司的一个操作环境。Dell PowerEdge Server BIOS 是一款系统更新驱动程序。DELL EMC PowerScale 是一套适用于非结构化数据的横向扩展存储系统。Dell EMC NetWorker 是一套统一备份和恢复软件。该软件提供备份与恢复、消除重复数据、备份报告等功能。DELL Dell Wyse Management Suite 是一套用于管理和优化 Wyse 端点的、可扩展的解决方案。该产品包括 Wyse 端点集中管理、资产追踪和自动设备发现等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞越权访问或者覆盖敏感数据，提升其权限，执行命令等。

CNVD 收录的相关漏洞包括：Dell Vnx2Oe For File 路径遍历漏洞、Dell OpenManage Enterprise 权限提升漏洞（CNVD-2022-42737）、DELL EMC AppSync 路径遍历漏洞、Dell VNX2 OE for File 远程代码执行漏洞（CNVD-2022-42739）、Dell PowerEdge 缓冲区溢出漏洞、DELL EMC PowerScale 代码问题漏洞、Dell EMC NetWorker 信息泄露漏洞（CNVD-2022-42743）、Dell Wyse Device Agent 授权问题漏洞。其中，“Dell OpenManage Enterprise 权限提升漏洞（CNVD-2022-42737）、Dell VNX2 OE for File 远程代码执行漏洞（CNVD-2022-42739）、Dell PowerEdge 缓冲区溢出漏洞”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-2022-42738

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42737

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42740

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42739

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42745

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42744

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42743

https://www.cnvd.org.cn/flaw/show/CNVD-2022-42742

5、Asus DSL-N14U-B1 拒绝服务漏洞

ASUS DSL-N14U-B1 是中国华硕（ASUS）公司的一款路由器设备。本周，ASUS DSL-N14U-B1 被披露存在拒绝服务漏洞。攻击者可利用该漏洞使用 nmap 之类的工具执行 TCP SYN 扫描造成拒绝服务 (DoS)。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-2022-41786

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-2022-42156	D-Link DIR882 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.dlink.com/en/security-bulletin/
CNVD-2022-42734	TOTOLINK A3100R setUrlFilterRules 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/170/ids/36.html
CNVD-2022-42733	TOTOLINK A3100R setportforwarrules 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/170/ids/36.html
CNVD-2022-42732	TOTOLINK A3100R setParentalRules 函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/170/ids/36.html
CNVD-2022-43094	Atlassian Confluence Server 和 Data Center 远程代码执行漏洞	高	官方已发布最新版本，建议受影响的用户及时更新升级到最新版本：https://www.atlassian.com/software/confluence/download-archives
CNVD-2022-43202	多款 Adobe 产品资源管理错误漏洞（CNVD-2022-43202）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-43204	多款 Adobe 产品资源管理错误漏洞（CNVD-2022-43204）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

			https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-43203	多款 Adobe 产品越界读取漏洞（CNVD-2022-43203）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-43209	多款 Adobe 产品资源管理错误漏洞（CNVD-2022-43209）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-43208	多款 Adobe 产品堆缓冲区溢出漏洞（CNVD-2022-43208）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://helpx.adobe.com/security/products/acrobat/apsb22-16.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。此外，Google、WordPress、Dell 等多款产品被披露存在多个漏洞，攻击者可利用漏洞越权访问或者覆盖敏感数据，提升其权限，执行命令，执行 SQL 注入攻击，删除缓存，删除源，创建源，上传恶意文件从而远程执行任意代码等。另外，ASUS DSL-N14U-B1 被披露存在拒绝服务漏洞。攻击者可利用该漏洞使用 nmap 之类的工具执行 TCP SYN 扫描造成拒绝服务 (DoS)。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、D-Link DIR-816 A2 命令注入漏洞

验证描述

D-Link DIR-816 A2 是中国台湾友讯（D-Link）公司的一款无线路由器。

D-Link DIR-816 A2 1.10 B05 存在命令注入漏洞，攻击者可利用该漏洞通过制作的 tokenid 参数任意重置设备到/goform/form2Reboot.cgi。

验证信息

POC 链接：https://github.com/GD008/vuln/blob/main/DIR-816_reset.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-42154

信息提供者

新华三技术有限公司

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. GitLab 通过安全更新修复了帐户接管漏洞

据 Bleeping Computer 网站 6 月 3 日消息，GitLab 为其社区版和企业版产品的多个版本发布了安全更新，以解决 8 个漏洞问题，其中一个为账户接管的漏洞。

参考链接：https://www.freebuf.com/news/335291.html

2. 紫光展锐曝漏洞，可阻止手机联网

据快科技报道，紫光展锐芯片组基带处理器被曝存在一个漏洞。由于该漏洞出现在芯片层，且直接负责网络连接的网络解调器，因此，攻击者通过该漏洞向用户发送损坏的数据包，可中断或禁止目标设备的网络连接。

参考链接：https://www.freebuf.com/news/335294.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