国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 11 月 11 日-2024 年 11 月 17 日　　2024 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 420 个，其中高危漏洞 228 个、中危漏洞 167 个、低危漏洞 25 个。漏洞平均分值为 6.64。本周收录的漏洞中，涉及 0day 漏洞 310 个（占 74%），其中互联网上出现“SimpCMS 跨站脚本漏洞、DedeCMS 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漏洞总数 19639 个，与上周（6618 个）环比增加 197%。

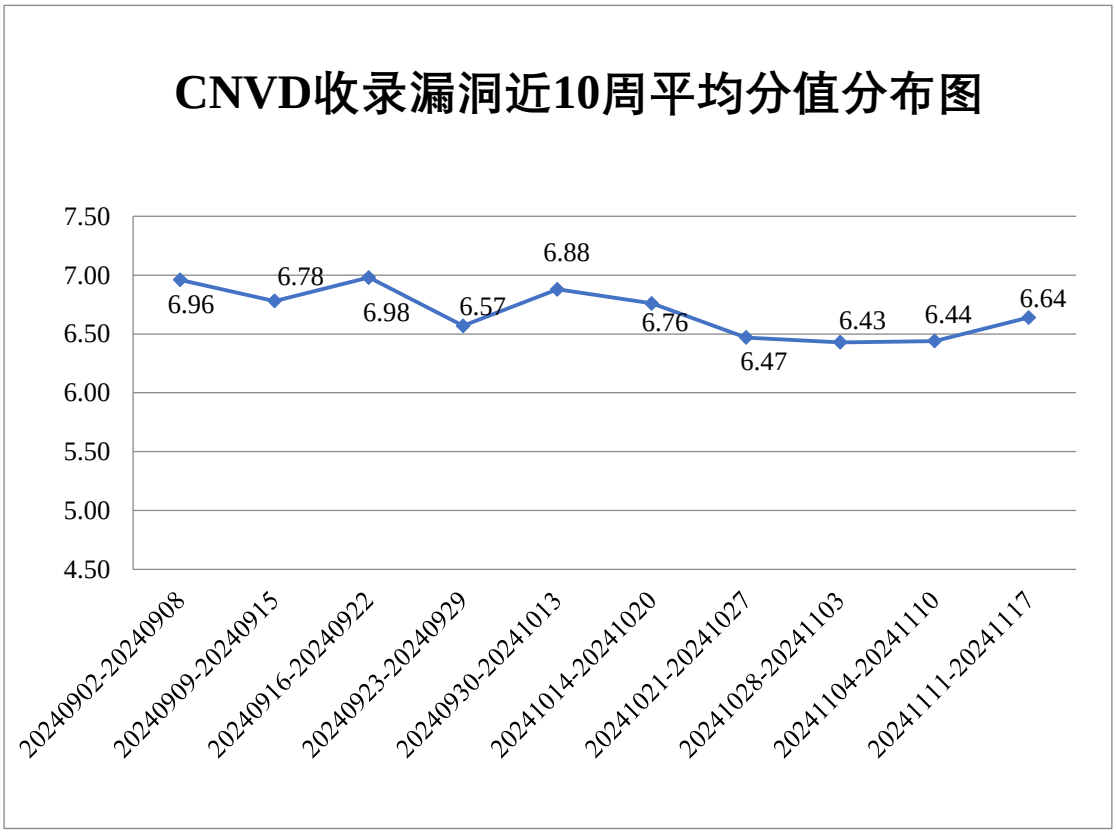

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 5 起，向基础电信企业通报漏洞事件 7 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 1176 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 73 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 22 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：

重庆朗奕迪实业有限公司、中科方德软件有限公司、郑州金鼓通信技术有限公司、浙江网盛生意宝股份有限公司、用友网络科技股份有限公司、信呼、西门子（中国）有限公司、西安紫云羚网络科技有限责任公司、武汉金同方科技有限公司、无锡信捷电气股份有限公司、同方知网（北京）技术有限公司、师创教育软件研究院（江苏）有限公司、深圳誉龙数字技术有限公司、深圳市有为信息技术发展有限公司、深圳市思迅软件股份有限公司、深圳市瑞驰信息技术有限公司、深圳市锐明技术股份有限公司、深圳市玛威尔显控科技有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市道尔智控科技股份有限公司、深圳市必联电子有限公司、深圳勤杰软件有限公司、熵基科技股份有限公司、厦门四信通信科技有限公司、厦门四联信息技术有限公司、厦门科拓通讯技术股份有限公司、厦门傲博教育科技有限公司、润申标准化技术服务（上海）有限公司、瑞斯康达科技发展股份有限公司、青岛东软载波科技股份有限公司、麒麟软件有限公司、力合科技（湖南）股份有限公司、蓝网科技股份有限公司、科亚医疗科技股份有限公司、江苏中安联科信息技术有限公司、吉翁电子（深圳）有限公司、吉林省启承网络科技有限公司、湖南众合百易信息技术有限公司、河南航天金穗电子有限公司、杭州云谷科技股份有限公司、杭州映云科技有限公司、杭州立方控股股份有限公司、汉王科技股份有限公司、海通安恒科技股份有限公司、广州云新信息技术有限公司、广州图创计算机软件开发有限公司、广州青鹿教育科技有限公司、广东飞企互联科技股份有限公司、广东保伦电子股份有限公司、泛微网络科技股份有限公司、东芝（中国）有限公司、点都互联科技有限公司、成都零起飞科技有限公司、畅捷通信息技术股份有限公司、北京紫荆云视科技有限公司、北京致远互联软件股份有限公司、北京英华在线科技有限公司、北京易普行科技有限公司、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、北京网动网络科技股份有限公司、北京神州视翰科技有限公司、北京勤云科技发展有限公司、北京凯特伟业科技有限公司、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京弘文恒瑞文化传播有限公司、北京北大方正电子有限公司、安科瑞电气股份有限公司和 Axis Communications AB。

本周，CNVD 发布了《关于新增快页信息技术有限公司等八家单位为 CNVD 支撑单位的公告》，详情参见 CNVD 网站公告内容（https://www.cnvd.org.cn/webinfo/show/10651）。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天津市国瑞数码安全系统股份有限公司、北京启明星辰信息安全技术有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。河南东方云盾信息技术有限公司、成都卫士通信息安全技术有限公司、江苏云天网络安全技术有限公司、江苏金盾检测技术股份有限公司、北京中睿天下信息技术有限公司、江苏正信信息安全测试有限公司、北京时代新威信息技术有限公司、北京航空航天大学、吉林省吉林祥云信息技术有限公司、星云博创科技有限公司、贵州多彩网安科技有限公司、中孚安全技术有限公司及其他个人白帽子向 CNVD 提交了 19639 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）、三六零数字安全科技集团有限公司、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 19267 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）	17458	17458
天津市国瑞数码安全系统股份有限公司	1953	0
北京启明星辰信息安全技术有限公司	1184	0
新华三技术有限公司	1101	0
三六零数字安全科技集团有限公司	802	802
上海交大	657	657
北京神州绿盟科技有限公司	463	43
奇安信网神（补天平台）	350	350
安天科技集团股份有限公司	303	0
北京天融信网络安全技术有限公司	209	10
杭州安恒信息技术股份有限公司	203	0
深信服科技股份有限	199	0

公司		
北京知道创宇信息技术有限公司	107	0
南京众智维信息科技有限公司	96	2
北京数字观星科技有限公司	26	0
北京升鑫网络科技有限公司（青藤云）	25	25
远江盛邦（北京）网络安全科技股份有限公司	22	22
厦门服云信息科技有限公司	19	0
北京长亭科技有限公司	13	0
杭州迪普科技股份有限公司	12	1
北京安信天行科技有限公司	10	10
快页信息技术有限公司	9	9
河南东方云盾信息技术有限公司	47	47
成都卫士通信息安全技术有限公司	27	27
西门子（中国）有限公司	26	0
江苏云天网络安全技术有限公司	11	11
江苏金盾检测技术股份有限公司	10	10
北京中睿天下信息技术有限公司	6	6
江苏正信信息安全测	2	2

试有限公司		
北京时代新威信息技术有限公司	2	2
北京航空航天大学	2	2
吉林省吉林祥云信息技术有限公司	1	1
星云博创科技有限公司	1	1
贵州多彩网安科技有限公司	1	1
中孚安全技术有限公司	1	1
个人	139	139
报送总计	25497	19639

本周漏洞按类型和厂商统计

本周，CNVD 收录了 420 个漏洞。WEB 应用 212 个，网络设备（交换机、路由器等网络端设备）100 个，应用程序 78 个，智能设备（物联网终端设备）15 个，安全产品 7 个，操作系统 5 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	212
网络设备（交换机、路由器等网络端设备）	100
应用程序	78
智能设备（物联网终端设备）	15
安全产品	7
操作系统	5
数据库	3

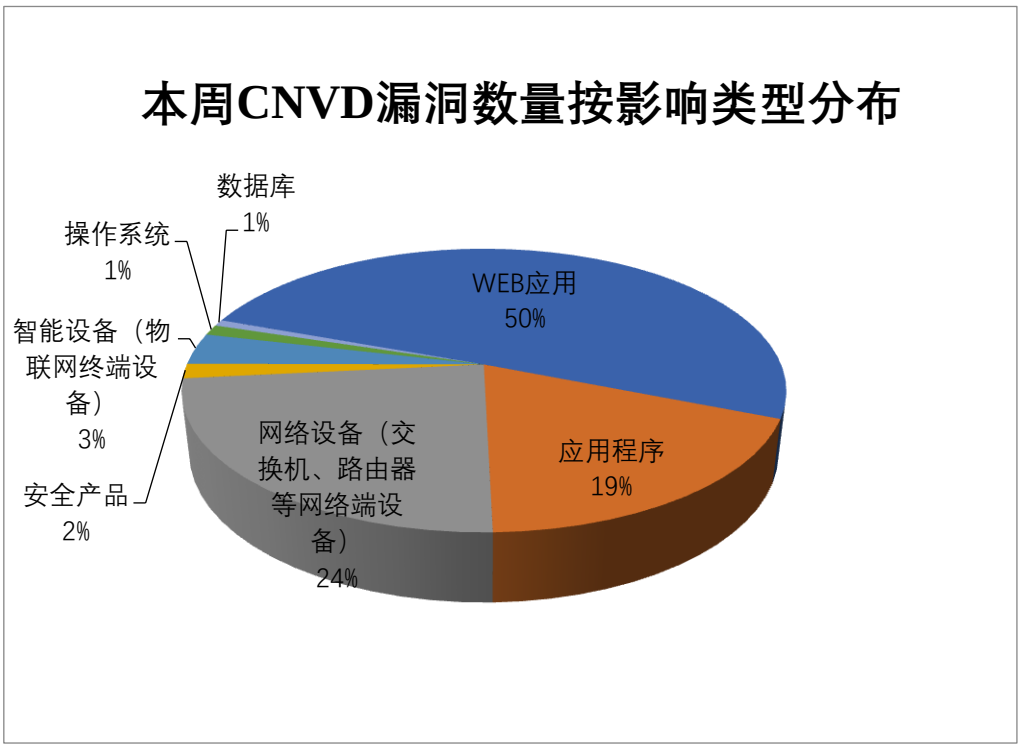

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Google、畅捷通信息技术股份有限公司等多家厂商的产品，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	Adobe	19	5%
2	Google	18	4%
3	畅捷通信息技术股份有限公司	13	3%
4	深圳市吉祥腾达科技有限公司	13	3%
5	用友网络科技股份有限公司	12	3%
6	NETGEAR	11	3%
7	Tenda	11	3%
8	D-Link	10	2%
9	Cisco	10	2%
10	其他	303	72%

本周行业漏洞收录情况

本周，CNVD 收录了 64 个电信行业漏洞，6 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Tenda AC10 缓冲区溢出漏洞（CNVD-2024-44853）、

Siemens SIMATIC CP 1543-1 授权错误漏洞”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/

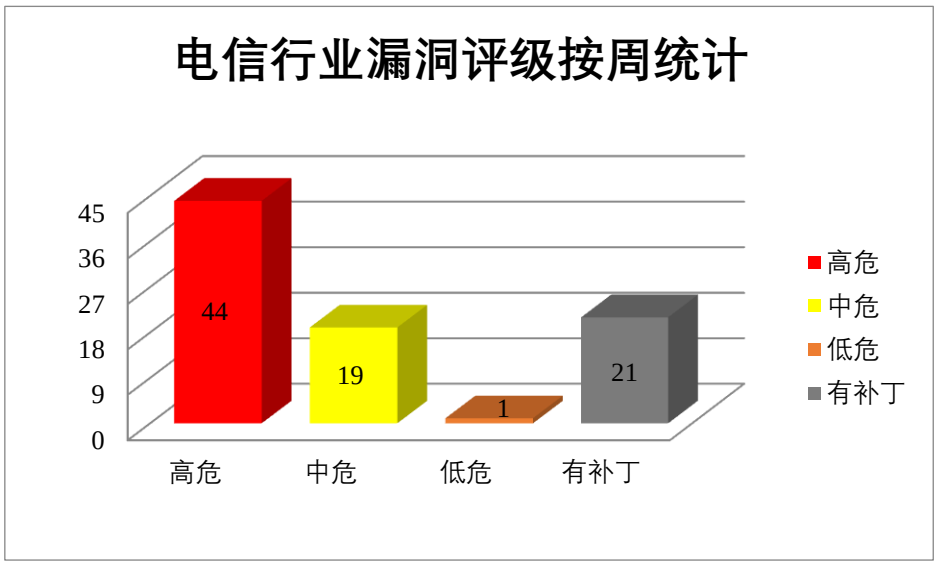

图 3 电信行业漏洞统计

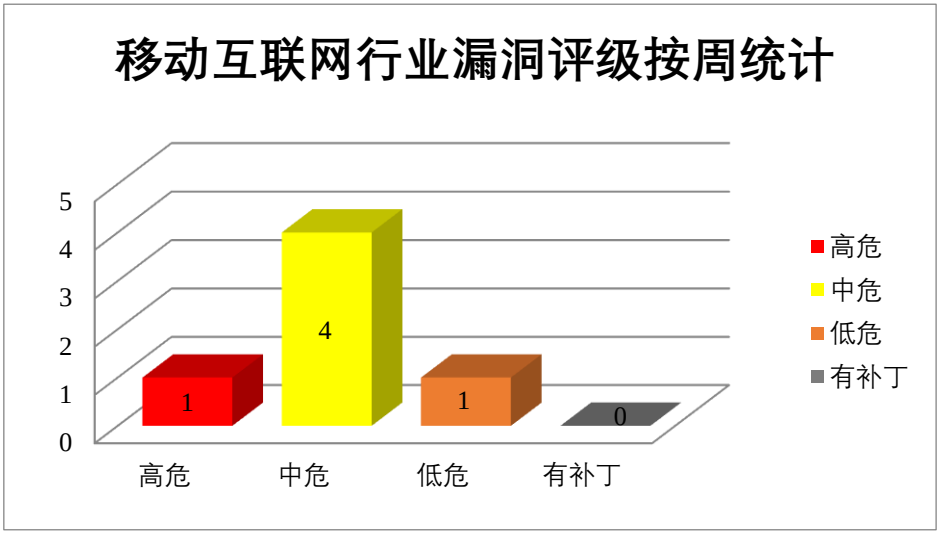

图 4 移动互联网行业漏洞统计

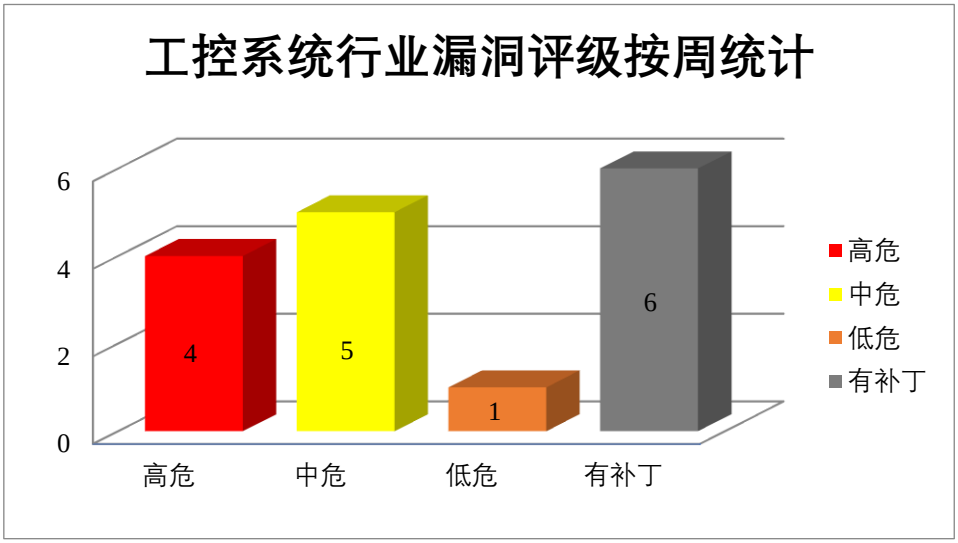

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft Outlook 是美国微软（Microsoft）公司的一套电子邮件应用程序。Microsoft Visual Studio 是一款开发工具套件系列产品，也是一个基本完整的开发工具集，它包括了整个软件生命周期中所需要的大部分工具。Microsoft .NET 是一个致力于敏捷软件开发、快速应用开发、平台无关性和网络透明化的软件框架。Microsoft Azure Command Line Integration（CLI）是美国微软（Microsoft）公司的一个跨平台的命令行工具，可连接到 Azure 并对 Azure 资源执行管理命令。Microsoft Azure Monitor Agent 是一个轻量级代理程序，可安装在 Azure 或本地环境中的服务器或虚拟机上。Microsoft DeepSpeed 是美国微软（Microsoft）公司的一款易于使用的深度学习优化软件套件，可为 DL 训练和推理提供前所未有的规模和速度。Microsoft OpenSSH 是美国微软（Microsoft）公司的一套用于安全访问远程计算机的连接工具。Microsoft SharePoint 是美国微软（Microsoft）公司的一套企业业务协作平台。该平台用于对业务信息进行整合，并能够共享工作、与他人协同工作、组织项目和工作组、搜索人员和信息。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行权限绕过，在系统上执行任意代码，获得更高的权限等。

CNVD 收录的相关漏洞包括：Microsoft Outlook for macOS 安全绕过漏洞、Microsoft .NET 和 Visual Studio 远程代码执行漏洞、Microsoft .NET 和 Visual Studio 拒绝服务漏洞、Microsoft Azure Command Line Integration（CLI）权限提升漏洞、Microsoft Azure Monitor Agent 权限提升漏洞、Microsoft DeepSpeed 远程代码执行漏洞、Microsoft OpenSSH for Windows 远程代码执行漏洞、Microsoft SharePoint 权限提升漏洞（C

NVD-2024-44526）。其中，除“Microsoft Outlook for macOS 安全绕过漏洞、Microsoft Azure Monitor Agent 权限提升漏洞、Microsoft SharePoint 权限提升漏洞（CNVD-2024-44526）”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-2024-44516
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44520
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44521
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44522
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44523
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44524
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44525
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44526

2、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，攻击者可利用漏洞通过特制的 HTML 页面执行越界内存访问，导致堆损坏，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome 越界写入漏洞（CNVD-2024-44477）、Google Chrome 释放后重用漏洞（CNVD-2024-44480、CNVD-2024-44478、CNVD-2024-44482、CNVD-2024-44481、CNVD-2024-44542）、Google Chrome 类型混淆漏洞（CNVD-2024-44540、CNVD-2024-44539）。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-2024-44477
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44480
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44478
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44482
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44481
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44540
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44539
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44542

3、Cisco 产品安全漏洞

Cisco Firepower Threat Defense（FTD）是美国思科（Cisco）公司的一套提供下一代防火墙服务的统一软件。Cisco Secure Firewall Management Center（FMC）是一个全面、集中化的管理平台，用于 Cisco 的网络安全解决方案。它提供了对防火墙、应用控制、入侵防御、URL 过滤和高级恶意软件防护的统一管理。Cisco Adaptive Security

Appliance (ASA) 是思科公司开发的一款综合性网络安全设备，提供防火墙、VPN、IPS 等安全功能。它支持物理和虚拟部署，能够适应不同规模网络的安全需求。Cisco Expressway Series 是美国思科（Cisco）公司的一款用于防火墙外访问设备的软件。该软件为防火墙外的用户提供了简单、高度安全的访问功能，帮助远程办公人员在他们选择的设备上更有效地工作。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过访问控制策略，使用静态凭据访问受影响的系统，在底层操作系统上执行任意命令等。

CNVD 收录的相关漏洞包括：Cisco Firepower Threat Defense 代码问题漏洞（CNVD-2024-44487）、Cisco Secure Firewall Management Center 命令执行漏洞、Cisco Secure Firewall Management Center 服务器端请求伪造漏洞、Cisco Firepower Threat Defense 信任管理问题漏洞、Cisco Secure Firewall Management Center SQL 注入漏洞、Cisco Adaptive Security Appliance SSH 远程命令注入漏洞、Cisco Secure Firewall Management Center 命令注入漏洞、Cisco Expressway Series 命令注入漏洞。其中，除“Cisco Firepower Threat Defense 代码问题漏洞（CNVD-2024-44487）、Cisco Secure Firewall Management Center 服务器端请求伪造漏洞、Cisco Expressway Series 命令注入漏洞”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-2024-44487
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44490
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44489
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44488
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44495
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44494
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44493
https://www.cnvd.org.cn/flaw/show/CNVD-2024-44496

4、 Adobe 产品安全漏洞

Adobe Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。该软件用于打印，签名和注释 PDF。Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的环境中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2024-44499、CNVD-2024-44498）、Adobe Commerce 操作系统命令注入漏洞（CNVD-2024-44502）、Adobe Acrobat Reader 资源管理错误漏洞（CNVD-2024-44501、CNVD-2024-44500、CNVD-2024-44505）、Adobe Acrobat Reader 输入验证错误漏洞（CNVD-2024-44504）、Adobe Commerce 文件上传漏洞（CNVD-2024-44503）。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-2024-44499

https://www.cnvd.org.cn/flaw/show/CNVD-2024-44498

https://www.cnvd.org.cn/flaw/show/CNVD-2024-44502

https://www.cnvd.org.cn/flaw/show/CNVD-2024-44501

https://www.cnvd.org.cn/flaw/show/CNVD-2024-44500

https://www.cnvd.org.cn/flaw/show/CNVD-2024-44504

https://www.cnvd.org.cn/flaw/show/CNVD-2024-44503

https://www.cnvd.org.cn/flaw/show/CNVD-2024-44505

5、TOTOLINK X18 命令注入漏洞

TOTOLINK X18 是中国吉翁电子（TOTOLINK）公司的一个网状路由器系统。本周，TOTOLINK X18 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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-2024-44851

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

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-2024-44470	Mozilla Firefox 竞态条件漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2024-53/
CNVD-2024-44850	Moodle SQL 注入漏洞（CNVD-2024-44850）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://moodle.org/mod/forum/discuss.php?d=461206
CNVD-2024-44920	Dell PowerProtect DD 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.dell.com/support/kbdoc/en-us/000245360/dsa-2024-424-security-update-for-dell-pdsa-2024-424-security-update-for-dell-powerprotect-dd-vulnerabilityowerprotect-dd-vulnerability
CNVD-2024-44818	D-Link DI-8003 dbsrv.asp 文件缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dlink.com.cn/techsupport/ProductInfo.aspx?m=DI-8003
CNVD-2024	Tenda AC10 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及

-44853	（CNVD-2024-44853）		时关注更新：https://www.tenda.com.cn/download/detail-3506.html
CNVD-2024-44935	多款 Siemens 产品注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-354112.html
CNVD-2024-44808	NETGEAR R8500 bsw_fix.cgi 组件命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.netgear.com/about/security/
CNVD-2024-44517	NETGEAR XR300 wiz_dyn.cgi 组件命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.netgear.com/about/security/
CNVD-2024-44862	Tenda AC6 缓冲区溢出漏洞（CNVD-2024-44862）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tendacn.com/download/detail-3794.html
CNVD-2024-44488	Cisco Firepower Threat Defense 信任管理问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞进行权限绕过，在系统上执行任意代码，获得更高的权限等。此外，Google、Cisco、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过特制的 HTML 页面执行越界内存访问，导致堆损坏，执行任意代码，绕过访问控制策略，使用静态凭据访问受影响的系统，在底层操作系统上执行任意命令等。另外，TOTOLINK X18 被披露存在命令注入漏洞。攻击者可利用漏洞导致任意命令执行。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、SimpCMS 跨站脚本漏洞

验证描述

SimpCMS 是一个基于 PureEdit 的易于使用的 CMS。

SimpCMS 0.1 版本存在跨站脚本漏洞，该漏洞源于应用对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过注入到/admin.php 的标题字段的精心设计的有效

负载执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://packetstormsecurity.com/files/179219

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-44515

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. 数百万个 Wordpress 安全插件存在漏洞

一个关键的身份验证旁路漏洞已经被发现，影响到“非常简单的安全性”(以前的“非常简单的 SSL”)的 WalPal 插件，包括免费版本和 Pro 版本。

参考链接：https://www.bleepingcomputer.com/news/security/security-plugin-flaw-in-millions-of-wordpress-sites-gives-admin-access/

2. Palo Alto Networks 确认存在新的防火墙 0day 漏洞

在告知客户正在调查有关新的防火墙远程代码执行漏洞后，Palo Alto Networks 于周五证实，一种新的 0day 漏洞正被用于攻击。

参考链接：https://thehackernews.com/2024/11/pan-os-firewall-vulnerability-under.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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国家网络安全漏洞库，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，是我国计算机网络应急处理体系中的牵头单位。

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