国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 04 月 05 日-2021 年 04 月 11 日　　2021 年第 14 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 671 个，其中高危漏洞 164 个、中危漏洞 405 个、低危漏洞 102 个。漏洞平均分值为 5.51。本周收录的漏洞中，涉及 0day 漏洞 424 个（占 63%），其中互联网上出现“Mblog 跨站脚本漏洞（CNVD-2021-26119）、 PbootCMS SQL 注入漏洞（CNVD-2021-26207）”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 3147 个，与上周（3125 个）环比增加 0.7%。

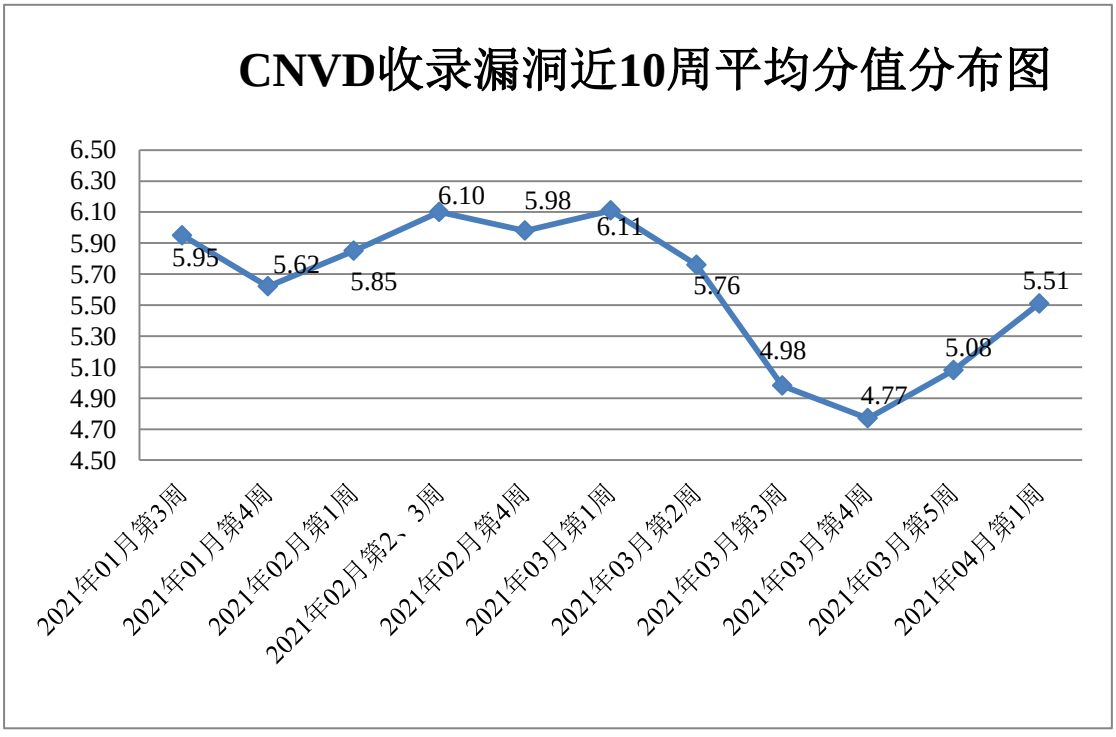

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 13 起，向基础电信企业通报漏洞事件 32 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 189 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 20 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 43 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、重庆朗奕迪实业有限公司、正方软件股份有限公司、浙江同花顺云软件有限公司、浙江省数字安全证书管理有限公司、浙江兰德纵横网络技术股份有限公司、浙江汇信科技有限公司、长沙米拓信息技术有限公司、长沙德尚网络科技有限公司、运城市盘石网络科技有限公司、优酷信息技术（北京）有限公司、用友网络科技股份有限公司、西安知先信息技术有限公司、西安锐通网络科技有限公司、微软（中国）有限公司、铜陵市金时代科技有限责任公司、深圳市圆梦云科技有限公司、深圳市英之杰网络科技有限公司、深圳市微笑智能有限公司、深圳市科脉技术股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳市朝恒辉网络科技有限公司、深圳昆仑通态科技有限责任公司、上海二三四五移动科技有限公司、熵基科技股份有限公司、厦门四信通信科技有限公司、锐捷网络股份有限公司、普联技术有限公司、南宁比优网络科技有限公司、南京品德科技有限责任公司、江苏仕德伟网络科技股份有限公司、湖北淘码千维信息科技有限公司、湖北点点点科技有限公司、弘扬软件股份有限公司、杭州荷花软件有限公司、汉王科技股份有限公司、海南赞赞网络科技有限公司、贵州亿垒科技有限公司、广州网易计算机系统有限公司、广州图创计算机软件开发有限公司、广东凯格科技有限公司、福建科立讯通信有限公司、福建福昕软件开发股份有限公司、烽火通信科技股份有限公司、东营金石软件有限公司、东莞市光速网络技术有限公司、成都万江港利科技有限公司、成都今网科技有限公司、博网追新科技（北京）有限公司、北京雄智伟业软件有限公司、北京微科通硕科技有限公司、北京国炬信息技术有限公司、北京东华原医疗设备有限责任公司、北京超图软件股份有限公司、北京百度网讯科技有限公司、安徽旭帆信息科技有限公司、安徽协达软件科技有限公司、安徽佰通教育科技发展有限公司、成都零起飞网络、易迅软件工作室、袁志蒙工作室、瓦房店市共济街道科创电脑服务中心、华夏 ERP、YYCMS、WordPress、SEMCMS、Seacms、Obra Soft、MongoDB、JPress、Dreamer CMS、CSZCMS、Catfish CMS、PDFTRON SYSTEMS, INC.和 Adobe。

本周，CNVD 发布了《关于亿邮电子邮件系统存在远程命令执行漏洞的安全公告》、《关于致远 OA 旧版本用户存在安全隐患应及时进行修复的风险提示》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6291

https://www.cnvd.org.cn/webinfo/show/6296

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、华为技术有限公司、国瑞数码零点实验室、厦门服云信息科技有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。北京信联科汇科技有限公司、杭州海康威视数字技术股份有限公司、南京众智维信息科技有限公司、河南信安世纪科技有限公司、浙江御安信息技术有限公司、上海纽盾科技股份有限公司、博智安全科技股份有限公司、山东华鲁科技发展股份有限公司、北京安帝科技有限公司、北京天地和兴科技有限公司、任子行网络技术股份有限公司、杭州木链物联网科技有限公司、北京安华金和科技有限公司、京东云安全、福建省海峡信息技术有限公司、河南灵创电子科技有限公司 、北京远禾科技有限公司、江苏智慧安全可信技术研究院、上海观安信息技术股份有限公司、北京君云天下科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、广州市云聚数据服务有限公司、海南神州希望网路有限公司、三一集团有限公司、山石网科通信技术股份有限公司、深圳市魔方安全科技有限公司、长春嘉诚信息技术股份有限公司、浙江乾冠信息安全研究院、中国银行及其他个人白帽子向 CNVD 提交了 3147 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 1050 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
上海交大	540	540
奇安信网神（补天平台）	323	323
斗象科技（漏洞盒子）	187	187
哈尔滨安天科技集团股份有限公司	180	0
华为技术有限公司	99	0
国瑞数码零点实验室	93	93
厦门服云信息科技有限公司	86	0
深信服科技股份有限公司	78	0
北京数字观星科技有限公司	70	0
北京神州绿盟科技有限公司	54	6
恒安嘉新（北京）科	54	0

技股份公司		
北京启明星辰信息安全技术有限公司	51	2
中国电信股份有限公司网络安全产品运营中心	32	12
远江盛邦（北京）网络安全科技股份有限公司	12	12
北京知道创宇信息技术股份有限公司	5	1
北京天融信网络安全技术有限公司	3	3
北京智游网安科技有限公司	1	1
内蒙古奥创科技有限公司	1	1
北京信联科汇科技有限公司	108	108
杭州海康威视数字技术股份有限公司	80	80
南京众智维信息科技有限公司	63	63
河南信安世纪科技有限公司	44	44
上海纽盾科技股份有限公司	15	15
博智安全科技股份有限公司	13	13
山东华鲁科技发展股份有限公司	12	12
北京安帝科技有限公司	12	12
北京天地和兴科技有限公司	11	11
浙江御安信息技术有限公司#4	20	20
任子行网络技术股份有限公司	11	11
杭州迪普科技股份有限公司	10	0
杭州木链物联网科技有限公司	7	7

北京安华金和科技有限公司	6	6
京东云安全	6	6
福建省海峡信息技术有限公司	4	4
河南灵创电子科技有限公司	3	3
北京远禾科技有限公司	2	2
江苏智慧安全可信技术研究院	2	2
上海观安信息技术股份有限公司	2	2
北京君云天下科技有限公司	1	1
北京云科安信科技有限公司（Seraph 安全实验室）	1	1
广州市云聚数据服务有限公司	1	1
海南神州希望网路有限公司	1	1
三一集团有限公司	1	1
山石网科通信技术股份有限公司	1	1
深圳市魔方安全科技有限公司	1	1
长春嘉诚信息技术股份有限公司	1	1
浙江乾冠信息安全研究院	1	1
中国银行	1	1
CNCERT 四川分中心	3	3
CNCERT 青海分中心	2	2
CNCERT 宁夏分中心	1	1
CNCERT 山东分中心	1	1
个人	1528	1528
报送总计	3845	3147

本周漏洞按类型和厂商统计

本周，CNVD 收录了 671 个漏洞。应用程序 306 个，WEB 应用 264 个，网络设备

（交换机、路由器等网络端设备）57 个，操作系统 20 个，安全产品 19 个，智能设备（物联网终端设备）4 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	306
WEB 应用	264
网络设备（交换机、路由器等网络端设备）	57
操作系统	20
安全产品	19
智能设备（物联网终端设备）	4
数据库	1

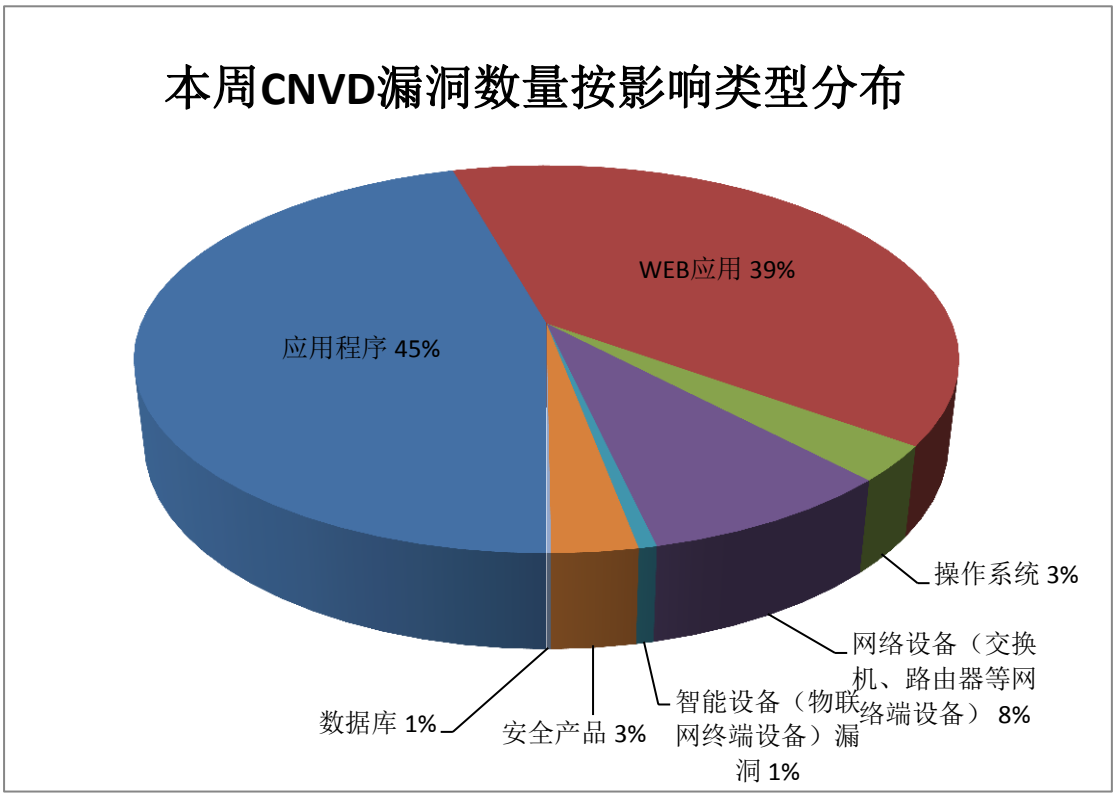

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 GitLab、Microsoft、上海孚盟软件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	GitLab	22	3%
2	Microsoft	21	3%
3	上海孚盟软件有限公司	19	3%
4	JerryScript	18	3%
5	TYPO3	15	2%
6	Foxit	14	2%

7	Adobe	13	2%
8	广东凯格科技有限公司	13	2%
9	CloudBees	11	2%
10	其他	525	78%

本周行业漏洞收录情况

本周，CNVD 收录了 40 个电信行业漏洞，27 个移动互联网行业漏洞，19 个工控行业漏洞（如下图所示）。其中，“多款 Schneider Electric 产品数据伪造问题漏洞、Rockwell Automation FactoryTalk AssetCentre SQL 注入漏洞（CNVD-2021-26399、CNVD-2021-26400、CNVD-2021-26401）、Rockwell Automation FactoryTalk AssetCentre OS 命令注入漏洞”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/

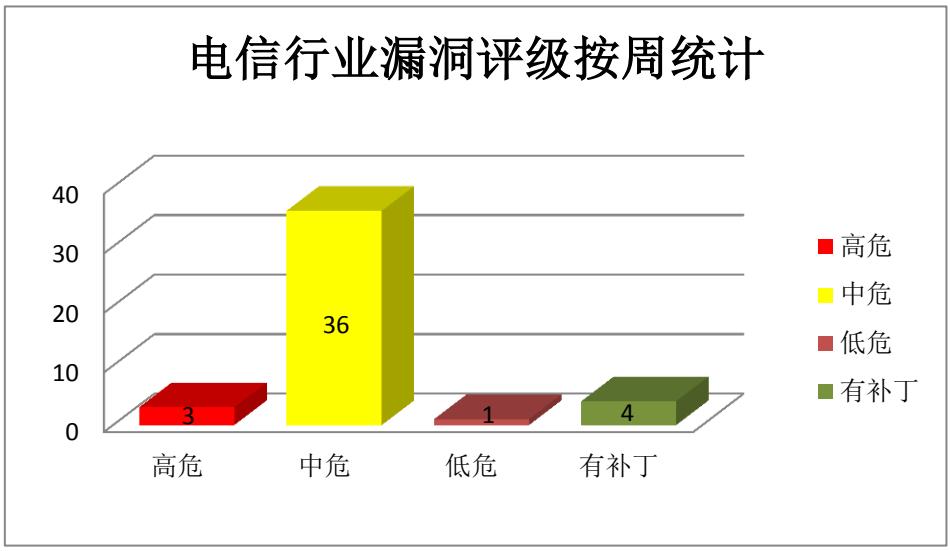

图 3 电信行业漏洞统计

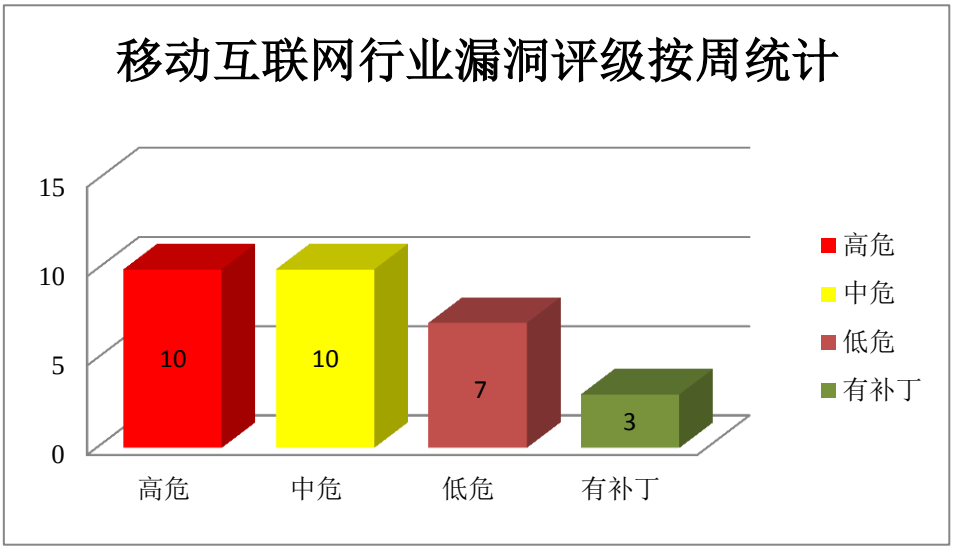

图 4 移动互联网行业漏洞统计

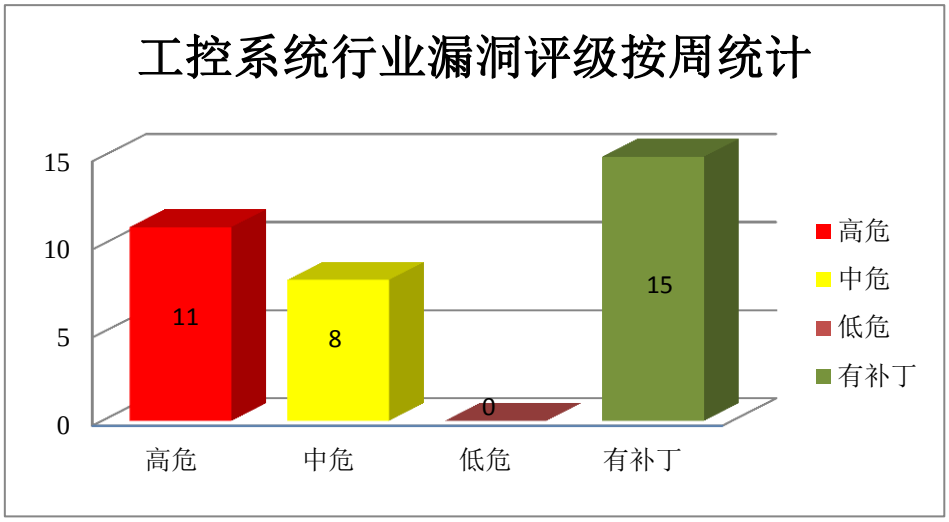

图 5 工控系统行业漏洞统计

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 Internet Explorer（IE）是美国微软（Microsoft）公司的一款 Windows 操作系统附带的 Web 浏览器。Microsoft Windows Defender 是美国微软（Microsoft）公司的一套 Windows 系统附带的防病毒软件。 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。Windows Graphics 是其中的一个图形组件。Microsoft Store Runtime 是美国微软（Microsoft）公司的一款应用商店软件。 Microsoft Outlook 是美国微软（Microsoft）公司的一套电子邮件应用程

序。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，导致内存损坏，删除系统上任意文件，在内核模式运行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft 浏览器内存损坏漏洞、Microsoft Windows Defender 权限提升漏洞（CNVD-2021-25012、CNVD-2021-25011）、Microsoft Windows 和 Microsoft Windows Server 权限提升漏洞（CNVD-2021-25977）、Microsoft Graphics 远程代码执行漏洞（CNVD-2021-26419）、Microsoft Outlook 安全功能绕过漏洞（CNVD-2021-25015）、Microsoft Store Runtime 权限提升漏洞（CNVD-2021-25014、CNVD-2021-25016）。其中“Microsoft 浏览器内存损坏漏洞、Microsoft Windows Defender 权限提升漏洞（CNVD-2021-25012、CNVD-2021-25011）、Microsoft Windows 和 Microsoft Windows Server 权限提升漏洞（CNVD-2021-25977）、Microsoft Graphics 远程代码执行漏洞（CNVD-2021-26419）”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-2021-25013

https://www.cnvd.org.cn/flaw/show/CNVD-2021-25012

https://www.cnvd.org.cn/flaw/show/CNVD-2021-25011

https://www.cnvd.org.cn/flaw/show/CNVD-2021-25977

https://www.cnvd.org.cn/flaw/show/CNVD-2021-26419

https://www.cnvd.org.cn/flaw/show/CNVD-2021-25016

https://www.cnvd.org.cn/flaw/show/CNVD-2021-25015

https://www.cnvd.org.cn/flaw/show/CNVD-2021-25014

2、Cisco 产品安全漏洞

Cisco Umbrella 是一个云安全平台，可提供抵御互联网威胁的第一道防线。Cisco Webex Meetings 提供了经济实惠的企业虚拟会议解决方案。Cisco IOS XR 软件是用于服务提供商网络的模块化和完全分布式的网络操作系统。Cisco Link Layer Discovery Protocol 是美国思科（Cisco）公司的一个路由器。Cisco Unified Communications Manager 是 Cisco 统一通信解决方案中强大的呼叫处理组件。它是一个可扩展、可分布、高度可用的企业 IP 语音呼叫处理解决方案。Cisco Unified Communications Manager Session Management Edition 是会话管理版。Cisco Unified Intelligence Center 是美国思科（Cisco）公司的一套基于 Web 的报表平台。该平台提供报告相关的业务数据和呼叫中心数据的展示功能。Cisco IOS XE 是针对未来工作进行优化的一个开放灵活的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞将恶意公式元素注入 CSV 文件，从而可操纵 CSV 文件中的数据或实现代码执行，诱使用户访问特制链接更改网页的内容，从而可将用户重定向到恶意网站，或进行进一步的客户端攻击，通过向受影响的命令提交特制输入以 root 权限在底层 Linux OS 上执行命令等。

CNVD 收录的相关漏洞包括：Cisco Umbrella CSV 公式注入漏洞、Cisco Webex

Meetings HTML 注入漏洞、Cisco IOS XR 命令注入漏洞、Cisco Link Layer Discovery Protocol 拒绝服务漏洞、Cisco Unified Communications Manager 信息泄露漏洞（CNVD-2021-26118）、Cisco Unified Communications Manager 授权绕过漏洞、Cisco Unified Intelligence Center 跨站脚本漏洞（CNVD-2021-26116）、Cisco IOS XE SD-WAN 命令注入漏洞。其中“Cisco IOS XE SD-WAN 命令注入漏洞”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-2021-26115
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26114
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26113
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26111
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26118
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26117
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26116
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26120

3、Foxit 产品安全漏洞

Foxit PhantomPDF 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，攻击者可利用漏洞在当前进程的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Foxit PhantomPDF 越界读取漏洞（CNVD-2021-26387、CNVD-2021-26386、CNVD-2021-26385、CNVD-2021-26390、CNVD-2021-26389、CNVD-2021-26388）、Foxit PhantomPDF 越界写入漏洞（CNVD-2021-26384）、Foxit PhantomPDF 内存错误引用漏洞（CNVD-2021-26392）。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-2021-26387
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26386
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26385
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26384
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26390
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26389
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26388
https://www.cnvd.org.cn/flaw/show/CNVD-2021-26392

4、CloudBees 产品安全漏洞

CloudBees Jenkins（Hudson Labs）是美国 CloudBees 公司的一套基于 Java 开发的持续集成工具。该产品主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞连接到攻击者指定的 U

RL，从而捕获 Jenkins 中存储的凭据，查看存储在 Jenkins 中的凭据的凭据 ID 等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins Team Foundation Server Plugin 授权不当漏洞（CNVD-2021-25258、CNVD-2021-25257）、CloudBees Jenkins Jabber Notifier and Control Plugin 跨站请求伪造漏洞、CloudBees Jenkins OWASP Dependency-Track Plugin 跨站请求伪造漏洞、CloudBees Jenkins OWASP Dependency-Track Plugin 授权不当漏洞、CloudBees Jenkins Team Foundation Server Plugin 跨站请求伪造漏洞、CloudBees Jenkins Build With Parameters Plugin 跨站请求伪造漏洞、CloudBees Jenkins Cloud Statistics Plugin 授权不当漏洞。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-2021-25257
https://www.cnvd.org.cn/flaw/show/CNVD-2021-25258
https://www.cnvd.org.cn/flaw/show/CNVD-2021-25262
https://www.cnvd.org.cn/flaw/show/CNVD-2021-25263
https://www.cnvd.org.cn/flaw/show/CNVD-2021-25260
https://www.cnvd.org.cn/flaw/show/CNVD-2021-25259
https://www.cnvd.org.cn/flaw/show/CNVD-2021-25265
https://www.cnvd.org.cn/flaw/show/CNVD-2021-25266

5、D-link DIR-816 A2 远程代码注入漏洞

D-link DIR-816 A2 是一款无线 AC750 双频路由器。本周，D-link DIR-816 A2 被披露存在远程代码注入漏洞。攻击者可利用漏洞通过 statuscheckpppoeuser 参数中的 shell 元字符利用该漏洞注入命令。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-2021-26374

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-2021-25268	Apache SpamAssassin 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://ubuntu.com/security/CVE-2020-1946
CNVD-2021-25270	Tobesoft Xplatform 代码执行漏洞（CNVD-2021-25270）	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.tobesoft.com/Index.do
CNVD-2021-25618	HGiga MailSherlock SQL 注入漏洞（CNVD-2021-25618）	高	厂商已发布了漏洞修复程序，请及时关注更新：

			http://www.hgiga.com/Product_MailSherlock.html
CNVD-2021-25683	Eclipse Jetty 拒绝服务漏洞（CNVD-2021-25683）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/eclipse/jetty.project/security/advisories/GHSA-26vr-8j45-3r4w
CNVD-2021-25687	Schneider Electric Unity Loader 和 OS Loader Software 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://www.se.com/ww/en/download/document/SEVD-2020-161-02/
CNVD-2021-25692	GOG Galaxy 权限许可和访问控制问题漏洞（CNVD-2021-25692）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.gog.com/
CNVD-2021-25695	Lansweeper 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.lansweeper.com/knowledgebase/restricting-access-to-the-web-console/
CNVD-2021-25698	Caddy 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/caddyserver/caddy/releases/tag/v0.10.13
CNVD-2021-25709	MyBB SQL 注入漏洞（CNVD-2021-25709）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/mybb/mybb/security/advisories/GHSA-r34m-ccm8-mfhq
CNVD-2021-25948	多款 Huawei 产品内存泄露漏洞（CNVD-2021-25948）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20210210-01-memoryleak-cn

小结：本周，Microsoft 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，导致内存损坏，删除系统上任意文件，在内核模式运行任意代码。此外，Cisco、Foxit、CloudBees 等多款产品被披露存在多个漏洞，攻击者可利用漏洞将恶意公式元素注入 CSV 文件，从而可操纵 CSV 文件中的数据或实现代码执行，诱使用户访问特制链接更改网页的内容，从而可将用户重定向到恶意网站，或进行进一步的客户端攻击，通过向受影响的命令提交特制输入以 root 权限在底层 Linux OS 上执行命令，在当前进程的上下文中执行任意代码，连接到攻击者指定的 URL，从而捕获 Jenkins 中存储的凭据，查看存储在 Jenkins 中的凭据的凭据 ID 等。另外，D-link DIR-816 A2 被披露存在远程代码注入漏洞。攻击者可利用漏洞通过 statuscheckpppoeuser 参数中的

shell 元字符利用该漏洞注入命令。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、Mblog 跨站脚本漏洞（CNVD-2021-26119）

验证描述

Mblog 是一款开源 Java 博客系统，支持多用户，支持切换主题。

Mblog 3.5.0 存在跨站脚本漏洞。攻击者可通过/post/editing 的 post header 字段利用该漏洞注入任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/langhsu/mblog/issues/27

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-26119

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. VMware 数据中心安全产品中发现严重漏洞

VMware 通报其 Carbon Black Cloud Workload 设备中有一个严重漏洞可以绕过身份验证并控制易受攻击的系统。漏洞编号为 CVE-2021-21982，在 CVSS 评分系统中，该漏洞的评分为 9.1，最高为 10。该漏洞会影响 1.0.1 之前的所有产品版本。

参考链接：https://thehackernews.com/2021/04/critical-auth-bypass-bug-found-in.html

2. SAP 系统安全补丁更新 72 小时内被活跃攻击

安全性 SAP 安全公司 Onapsis 警告说，在安全补丁发布后的 72 小时内，威胁行为者将本地 SAP 系统作为攻击目标。 根据 Onapsis 和 SAP 联合发表的一项研究，本地 SAP 系统受到威胁的威胁。

参考链接：https://thehackernews.com/2021/04/watch-out-mission-critical-sap.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