国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 03 月 08 日-2021 年 03 月 14 日　　2021 年第 10 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 617 个，其中高危漏洞 204 个、中危漏洞 267 个、低危漏洞 146 个。漏洞平均分值为 5.76。本周收录的漏洞中，涉及 0day 漏洞 386 个（占 63%），其中互联网上出现“Wordpress Hashtagger 插件跨站脚本漏洞、Maxum Rumpus 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 4752 个，与上周（6101 个）环比减少 22%。

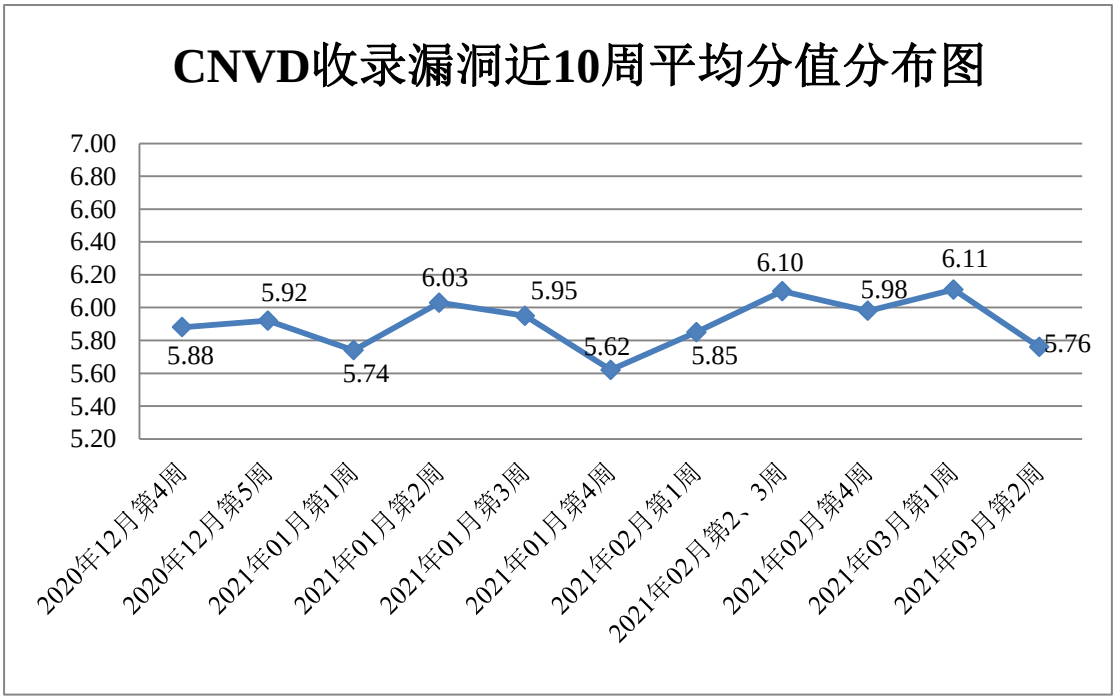

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 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 362 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 66 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 39 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：

暴风集团股份有限公司、金通证券有限责任公司、苏州科达科技股份有限公司、广州虎牙信息科技有限公司、联储证券有限责任公司、九州证券股份有限公司、万兴科技集团股份有限公司、东方财富证券股份有限公司、天风证券股份有限公司、新时代证券股份有限公司、北京火绒网络科技有限公司、深圳市华德安科技有限公司、民生证券股份有限公司、成都星锐蓝海网络科技有限公司、方正中期期货有限公司、深圳市房多多网络科技有限公司、北京海腾时代科技有限公司、江下信息科技（惠州）有限公司、上海二三四五移动科技有限公司、南京铱迅信息技术股份有限公司、北京启明星辰信息安全技术有限公司、廊坊市极致网络科技有限公司、微软（中国）有限公司、北京通达信科科技有限公司、浙江同花顺云软件有限公司、东北证券股份有限公司、大通证券股份有限公司、中邮证券有限责任公司、中国中金财富证券有限公司、三星（中国）投资有限公司、福建福昕软件开发股份有限公司、海南易而优科技有限公司、淄博闪灵网络科技有限公司、太平洋证券股份有限公司、锐捷网络股份有限公司、中国中信集团有限公司、世纪证券有限责任公司、上海嵩恒网络科技股份有限公司、广东熠鑫软件开发有限公司、北京西南偏南科技有限公司、河南青峰网络科技有限公司、华西期货有限责任公司、西南证券股份有限公司、申万宏源证券有限公司、金元证券股份有限公司、中信建投证券股份有限公司、北京猿力教育科技有限公司、咪咕视讯科技有限公司、北京云因信息技术有限公司、苏州开心盒子软件有限公司、用友网络科技股份有限公司、长沙米拓信息技术有限公司、北京华夏大地远程教育网络服务有限公司、成都润格无限科技有限公司、上海卓卓网络科技有限公司、北京网动网络科技股份有限公司、北京新东方迅程网络科技股份有限公司、北京视果科技有限公司、山西证券股份有限公司、五矿证券有限公司、英大证券有限责任公司、银泰证券有限责任公司、国联证券股份有限公司、宏信证券有限责任公司、广州思迈特软件有限公司、北京心更远科技发展有限公司、安徽旭帆信息科技有限公司、科大讯飞股份有限公司、长沙友点软件科技有限公司、北京米尔伟业科技公司、甬兴证券有限公司、钉钉（中国）信息技术有限公司、华宝证券有限责任公司、海通证券股份有限公司、红塔证券股份有限公司、华融证券股份有限公司、北京风行在线技术有限公司、邳州天目网络科技有限公司、惠普贸易（上海）有限公司、北京多点在线科技有限公司、青岛科创互联网络科技有限公司、深圳市网旭科技有限公司、津淳多媒體行銷有限公司、北京谋智火狐信息技术有限公司、上海互盾信息科技有限公司、深圳市汇佳互联科技有限公司、广州津虹网络传媒有限公司、南京九则软件科技有限公司、太原迅易科技有限公司、北京云帆互联科技有限公司、中控泰科（北京）

科技发展有限公司、北京百度网讯科技有限公司、成都奇鲁科技有限公司、四川盛趣时代网络科技有限公司、武汉斗鱼网络科技有限公司、广东一一五科技股份有限公司、深圳市锟铻科技有限公司、国晋信息科技有限公司、天津珊瑚信息科技有限公司、广联达科技股份有限公司、上海蓝山办公软件有限公司、紫光软件系统有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、广州红帆科技有限公司、沈阳点动科技有限公司、广州鼎成信息科技有限公司、葵花科技有限公司、北京百卓网络技术有限公司、北京爱奇艺科技有限公司、北京致远互联软件股份有限公司、畅捷通信息技术股份有限公司、东北师大理想软件股份有限公司、上海力软信息技术有限公司、阿里巴巴集团安全应急响应中心、上海商创网络科技、郑州沃龙建站、企炬中国、联想集团、若依、快转视频格式转换器鱼跃 CMS 、华夏 ERP、发货 100、JPress、WDJA、Ucms、YYCMS、115CMS、Oracle、FVC Studio、YZMCMS、Adobe、XIAOCMS 和 kitecms。

本周，CNVD 发布了《关于 Microsoft Exchange Server 存在多个高危漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6136

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、北京神州绿盟科技有限公司、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。南京众智维信息科技有限公司、山东云天安全技术有限公司、安徽长泰信息安全服务有限公司、北京信联科汇科技有限公司、江苏保旺达软件技术有限公司、山东泽鹿安全技术有限公司、河南灵创电子科技有限公司、上海犀点意象网络科技有限公司、河南信安世纪科技有限公司、北京天地和兴科技有限公司、山东华鲁科技发展股份有限公司、北京山石网科信息技术有限公司、贵州多彩宝互联网服务有限公司、北京安帝科技有限公司、北方实验室（沈阳）股份有限公司、京东云安全、武汉明嘉信信息安全检测评估有限公司、西安交大捷普网络科技有限公司、北京机沃科技有限公司、北京圣博润高新技术股份有限公司、上海峭函信息科技有限公司、广州安亿信软件科技有限公司、深圳市魔方安全科技有限公司、神州网安（北京）信息科技有限公司、上海纽盾科技股份有限公司、山东新潮信息技术有限公司、北京君云天下科技有限公司、杭州天谷信息科技有限公司、上海观安信息技术股份有限公司、广东蓝爵网络安全技术股份有限公司及其他个人白帽子向 CNVD 提交了 4752 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 3016 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

奇安信网神（补天平台）	2121	2121
斗象科技（漏洞盒子）	895	895
北京天融信网络安全技术有限公司	456	2
北京神州绿盟科技有限公司	283	133
哈尔滨安天科技集团股份有限公司	262	0
新华三技术有限公司	129	0
华为技术有限公司	123	0
深信服科技股份有限公司	79	0
北京奇虎科技有限公司	63	63
北京启明星辰信息安全技术有限公司	61	5
中国电信集团系统集成有限责任公司	39	39
中国电信股份有限公司网络安全产品运营中心	30	10
天津市国瑞数码安全系统股份有限公司	27	27
北京数字观星科技有限公司	15	0
远江盛邦（北京）网络安全科技股份有限公司	3	3
北京知道创宇信息技术股份有限公司	1	1
北京智游网安科技有限公司（爱加密）	1	1
南京众智维信息科技有限公司	163	163
山东云天安全技术有限公司	80	80
安徽长泰信息安全服务有限公司	55	55
北京信联科汇科技有限公司	49	49
江苏保旺达软件技术有限公司	40	40

山东泽鹿安全技术有限公司	39	39
河南灵创电子科技有限公司	27	27
上海犀点意象网络科技有限公司	24	24
西门子（中国）有限公司	24	0
河南信安世纪科技有限公司	23	23
北京天地和兴科技有限公司	20	20
杭州迪普科技股份有限公司	17	0
山东华鲁科技发展股份有限公司	15	15
北京山石网科信息技术有限公司	14	14
贵州多彩宝互联网服务有限公司	12	12
北京安帝科技有限公司	10	10
北方实验室（沈阳）股份有限公司	9	9
京东云安全	9	9
北京华顺信安科技有限公司	8	0
武汉明嘉信信息安全检测评估有限公司	7	7
西安交大捷普网络科技有限公司	6	6
北京机沃科技有限公司	4	4
北京圣博润高新技术股份有限公司	3	3
上海崤函信息科技有限公司	3	3
广州安亿信软件科技有限公司	2	2
深圳市魔方安全科技有限公司	2	2
神州网安（北京）信息科技有限公司	2	2
上海纽盾科技股份有限公司	2	2

山东新潮信息技术有限公司	1	1
北京君云天下科技有限公司	1	1
杭州天谷信息科技有限公司	1	1
上海观安信息技术股份有限公司	1	1
广东蓝爵网络安全技术股份有限公司	1	1
CNCERT 西藏分中心	3	3
CNCERT 青海分中心	2	2
CNCERT 四川分中心	2	2
CNCERT 山东分中心	1	1
个人	819	819
报送总计	6089	4752

本周漏洞按类型和厂商统计

本周，CNVD 收录了 617 个漏洞。应用程序 337 个，WEB 应用 215 个，网络设备（交换机、路由器等网络端设备）44 个，安全产品 7 个，操作系统 7 个，智能设备（物联网终端设备）4 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
应用程序	337
WEB 应用	215
网络设备（交换机、路由器等网络端设备）	44
安全产品	7
操作系统	7
智能设备（物联网终端设备）	4
数据库	3

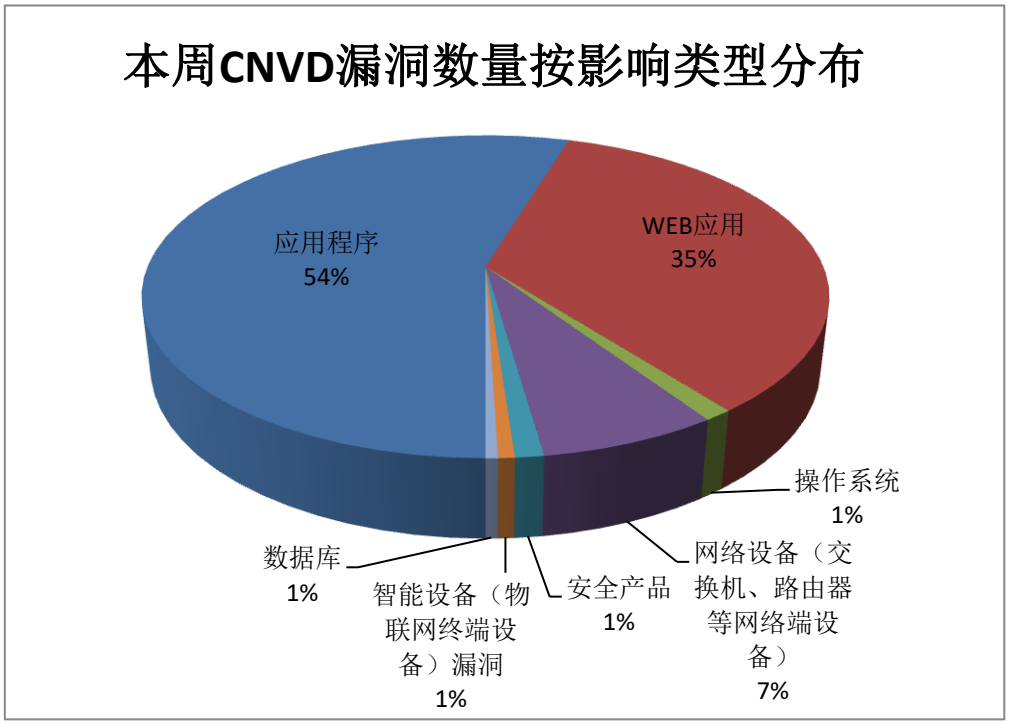

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、珠海金山办公软件有限公司、深圳市腾讯计算机系统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	Mozilla	32	5%
2	珠海金山办公软件有限公司	23	4%
3	深圳市腾讯计算机系统有限公司	21	4%
4	杭州奇亿云计算有限公司	16	3%
5	广州市创科网络科技有限公司	15	2%
6	Siemens	15	2%
7	MB CONNECT LINE	15	2%
8	上海装盟信息科技有限公司	15	2%
9	IBM	12	2%
10	其他	453	74%

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，39 个移动互联网行业漏洞，23 个工控行

业漏洞（如下图所示）。其中，“Siemens SCALANCE 和 RUGGEDCOM 设备拒绝服务漏洞、Siemens SIMATIC MV400 系列 TCP 协议栈安全特征问题漏洞、Cisco SD-WAN UDP 拒绝服务漏洞、Siemens SCALANCE 和 RuggedCmd 设备堆栈溢出漏洞”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/

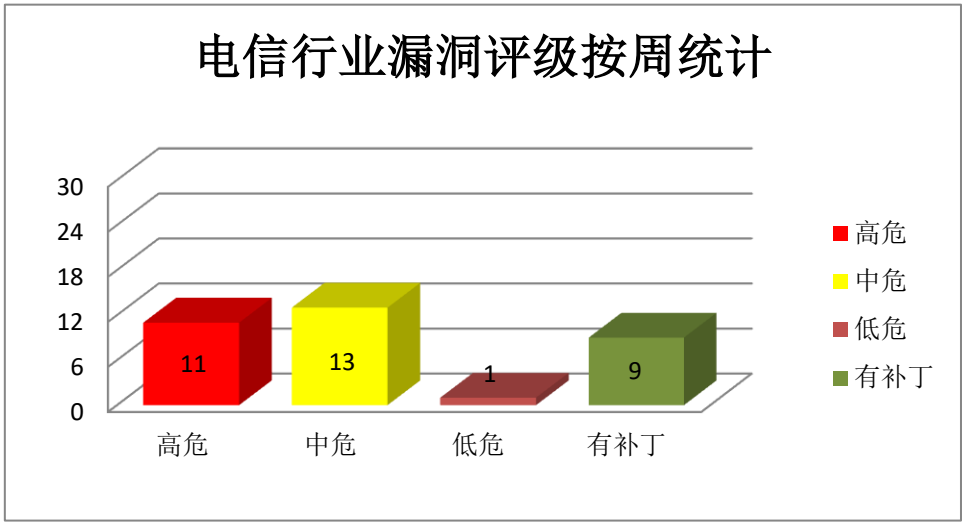

图 3 电信行业漏洞统计

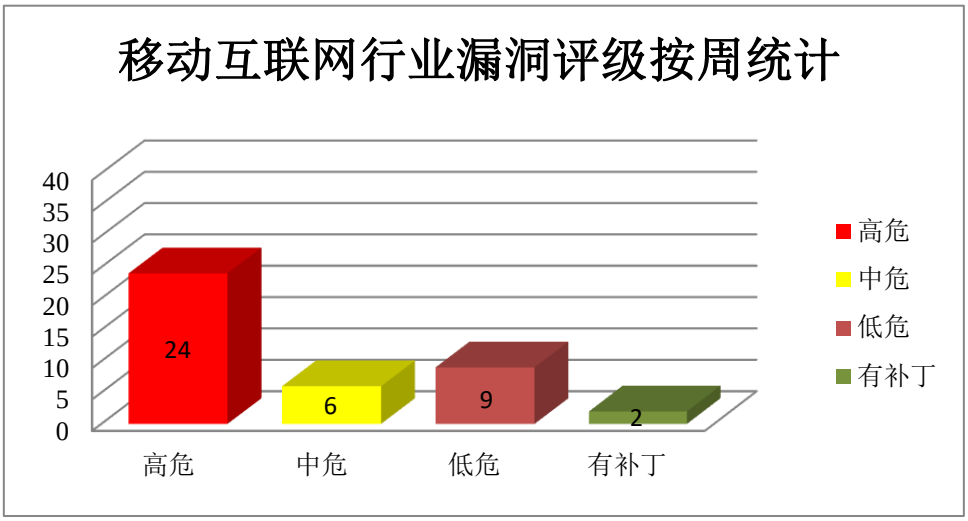

图 4 移动互联网行业漏洞统计

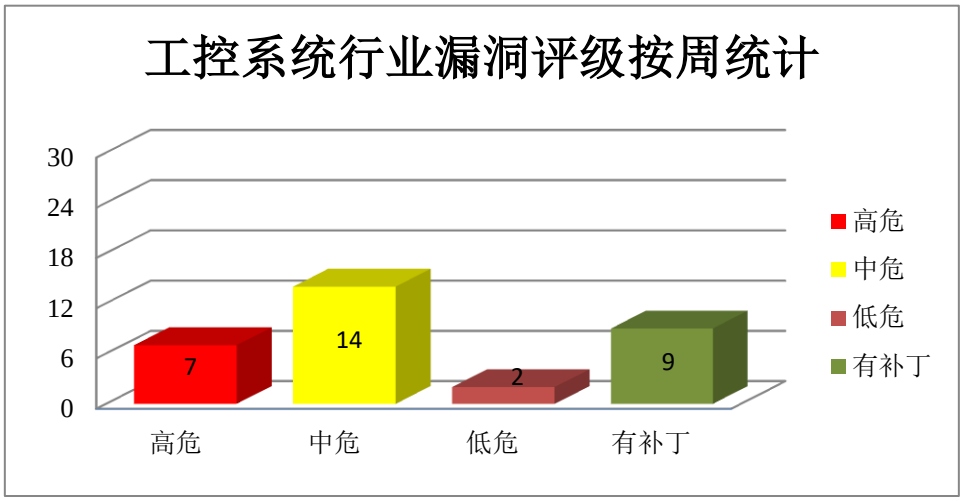

图 5 工控系统行业漏洞统计

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、 Siemens 产品安全漏洞

Siemens SINEMA Remote Connect Server 是一套远程网络管理平台。Siemens Solid Edge 是一款三维 CAD 软件。SIMATIC S7-PLCSIM V5.4 是一个 Windows 应用程序，它模拟用户程序的执行，用于模拟模拟 S7-300 CPU、S7-400 CPU 和 WinAC 系列控制器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取任意文件，在当前进程的上下文中执行代码，造成拒绝服务情况等。

CNVD 收录的相关漏洞包括：Siemens SINEMA Remote Connect Server 不正确授权漏洞（CNVD-2021-16437、CNVD-2021-16436）、Siemens Solid Edge 越界写入漏洞、Siemens Solid Edge XML 外部实体引用漏洞、Siemens Solid Edge 越界写入漏洞（CNVD-2021-16439）、Siemens Solid Edge 越界读取漏洞、Siemens SIMATIC S7-PLCSIM 拒绝服务漏洞、Siemens SIMATIC S7-PLCSIM 空指针取消引用漏洞。其中，除“Siemens Solid Edge XML 外部实体引用漏洞、Siemens SIMATIC S7-PLCSIM 拒绝服务漏洞、Siemens SIMATIC S7-PLCSIM 空指针取消引用漏洞”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-2021-16437

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16436

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16441

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16440

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16439

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16438

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16445

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16446

2、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息或劫持用户会话，可使应用程序崩溃或以应用程序上下文执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2021-15048、CNVD-2021-15498）、Mozilla Firefox 内存破坏代码执行漏洞（CNVD-2021-15495、CNVD-2021-15496、CNVD-2021-15500、CNVD-2021-15499）、Mozilla Firefox 点击劫持漏洞、Mozilla Firefox 跨站脚本漏洞（CNVD-2021-15502）。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-2021-15048

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15498

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15495

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15496

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15500

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15499

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15497

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15502

3、Aruba Networks 产品安全漏洞

Aruba Networks AirWave Management Platform 是一套适用于多供应商管理的网络管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取和修改底层数据库中的敏感信息，执行任意命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Aruba Networks AirWave Management Platform 命令注入漏洞（CNVD-2021-15033、CNVD-2021-15041、CNVD-2021-15042、CNVD-2021-15035）、Aruba Networks AirWave Management Platform SQL 注入漏洞（CNVD-2021-15037、CNVD-2021-15036）、Aruba Networks AirWave Management Platform 不当访问控制漏洞、Aruba Networks AirWave Management Platform XML 外部实体注入漏洞。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-2021-15033

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15041

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15042

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15035

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15037

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15036

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15034

https://www.cnvd.org.cn/flaw/show/CNVD-2021-15042

4、SAP 产品安全漏洞

SAP 3D Visual Enterprise Viewer 是一款适用于 Windows 的免费 3D 可视化查看器。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞导致程序崩溃。

CNVD 收录的相关漏洞包括：SAP 3D Visual Enterprise Viewer 拒绝服务漏洞（CNVD-2021-16366、CNVD-2021-16369、CNVD-2021-16368、CNVD-2021-16367、CNVD-2021-16370、CNVD-2021-16932、CNVD-2021-16931、CNVD-2021-16930）。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-2021-16366

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16369

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16368

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16367

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16370

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16932

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16931

https://www.cnvd.org.cn/flaw/show/CNVD-2021-16930

5、Delta Electronics CNCSoft-B 缓冲区溢出漏洞

Delta Electronics CNCSoft-B 是一款数控机床仿真系统软件。本周，Delta Electronics CNCSoft-B 被披露存在缓冲区溢出漏洞。该漏洞源于空指针错误，攻击者可利用该漏洞执行任意代码。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-2021-17271

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-2021-15052	Visualware MyConnection Server 文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://packetstormsecurity.com/files/161571/VisualWare-MyConnection-Server-11.x-Remote-Code-Execution.html

CNVD-2021-15488	Secomea GateManager 文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.secomea.com/support/cybersecurity-advisory/#3737
CNVD-2021-16596	Cisco SD-WAN CLI 命令注入漏洞（NVD-C-2021-20070）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgc
CNVD-2021-17195	F5 BIG-IP HTTP 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K02333782
CNVD-2021-17192	IBM DB2 缓冲区溢出漏洞（CNVD-2021-17192）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/6427855
CNVD-2021-17201	FUEL CMS SQL 注入漏洞（CNVD-2021-17201）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/daylightstudio/FUEL-CMS/commit/47303d707a34e5818724e3124421a9ea6ac6753b
CNVD-2021-17222	Trend Micro Virus Scan API 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://success.trendmicro.com/solution/000285675
CNVD-2021-17227	Cisco NX-OS Software 任意文件操作漏洞	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-3000-9000-fileaction-QtLzDRy2
CNVD-2021-17226	ImageMagick ImplodeImage 拒绝服务漏洞（CNVD-2021-17226）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugzilla.redhat.com/show_bug.cgi?id=1928959
CNVD-2021-17230	IBM Workload Automation 信息泄露漏洞（CNVD-2021-17230）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/6402483

小结：本周，Siemens 产品被披露存在多个漏洞，攻击者可利用漏洞获取任意文件，在当前进程的上下文中执行代码，造成拒绝服务情况等。此外，Mozilla、Aruba Networks、SAP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息或劫持用户会话，执行任意命令，导致拒绝服务等。另外，Delta Electronics CNCSoft-B 被披露存在缓冲区

溢出漏洞。攻击者可利用该漏洞执行任意代码。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 Hashtagger 插件跨站脚本漏洞

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 Hashtagger 插件存在跨站脚本漏洞，该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2021010092

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-17252

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. F5 警告：Big-IP 版本中发现严重的预授权漏洞

应用安全公司 F5 在 10 日发布警告，Big-IP 版本中发现了四个严重级别的漏洞，可能导致拒绝服务攻击及未经身份验证的远程代码执行。

参考链接：https://thehackernews.com/2021/03/critical-pre-auth-rce-flaw-found-in-f5.html

2. 研究人员发现插件中的零日漏洞，可接管 WordPress 网站

Wordfence 团队研究人员 10 日表示，在 The Plus Addons for Elementor WordPress 插件中发现了一个零日漏洞漏洞，可以利用该漏洞获得网站管理权并接管网站。研究人员警告，该零日漏洞已在野利用。

参考链接：https://securityaffairs.co/wordpress/115451/hacking/the-plus-addons-for-elementor-wordpress-flaw.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