国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 07 月 12 日-2021 年 07 月 18 日　　2021 年第 28 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 575 个，其中高危漏洞 158 个、中危漏洞 348 个、低危漏洞 69 个。漏洞平均分值为 5.65。本周收录的漏洞中，涉及 0day 漏洞 360 个（占 63%），其中互联网上出现“dotCMS 跨站脚本漏洞（CNVD-2021-50940）、Halo 服务器端请求伪造漏洞”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 4147 个，与上周（4773 个）环比减少 13%。

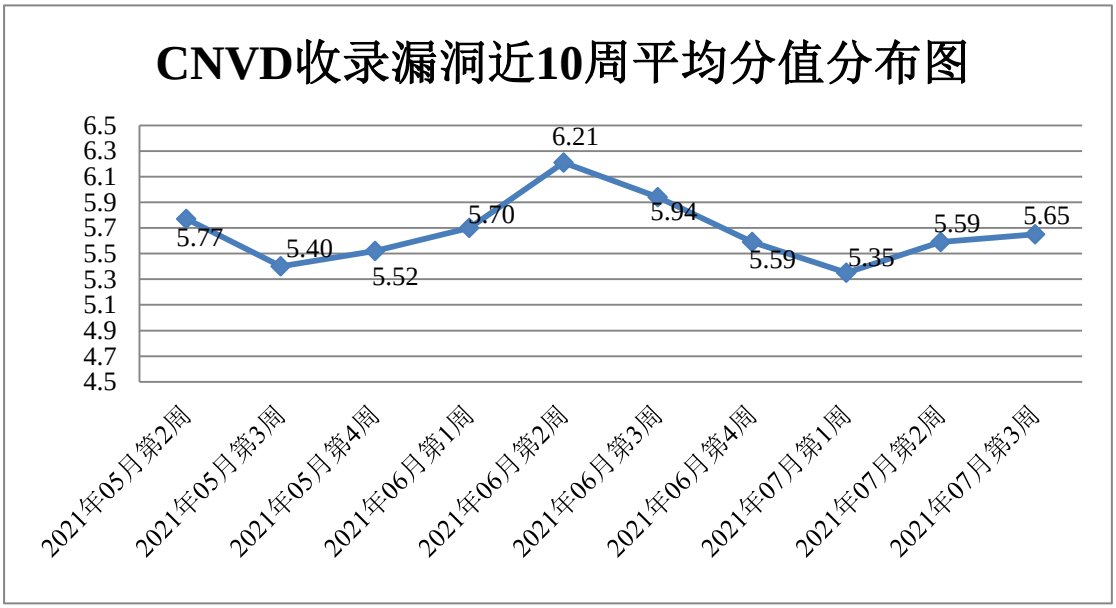

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 起，向基础电信企业通报漏洞事件 39 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 346 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 27 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 51 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：

作业帮教育科技（北京）有限公司、紫光软件系统有限公司、珠海玖时光科技有限公司、重庆中联信息产业有限责任公司、中兴通讯股份有限公司、中科博华信息科技有限公司、中孚信息股份有限公司、郑州天迈科技股份有限公司、浙江鼎成网络有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、友讯电子设备（上海）有限公司、夏普商贸（中国）有限公司、西门子（中国）有限公司、西安启莱软件科技有限公司、潍坊家园驿站电子技术有限公司、微软（中国）有限公司、微宏软件技术（杭州）有限公司、天闻数媒科技（北京）有限公司、天津神州浩天科技有限公司、苏州科达科技股份有限公司、苏州国网电子科技有限公司、苏宁易购集团股份有限公司、松下电器（中国）有限公司、四川易瑞特科技有限公司、守内安信息科技（上海）有限公司、深圳市子辰视讯科技有限公司、深圳市中科网威科技有限公司、上海艾泰科技有限公司、深圳维盟科技股份有限公司、北京信达网安科技有限公司、广州同聚成电子科技有限公司、深圳市网域科技股份有限公司、深圳市利谱信息技术有限公司、北京瑞星网安技术股份有限公司、北京华清信安科技有限公司、深圳华域数安科技有限公司、北京华御科技有限公司、深圳市因格智能科技有限公司、深圳市图美电子技术有限公司、深圳市锟铻科技有限公司、深圳市科脉技术股份有限公司、深圳市吉祥腾达科技有限公司、深圳市百为通达科技有限公司、上海尊蓝信息科技发展股份有限公司、上海知汇云信息技术股份有限公司、上海焱凤信息技术有限公司、上海七慧网络科技有限公司、上海穆云智能科技有限公司、上海宽娱数码科技有限公司、上海泛微网络科技股份有限公司、上海创图网络科技股份有限公司、上海博瑞康数字科技有限公司、熵基科技股份有限公司、陕西硅峰网络科技有限公司、山东思达特测控设备有限公司、山东国子软件股份有限公司、厦门市灵鹿谷科技有限公司、普联技术有限公司、南通润邦网络科技有限公司、南宁比优网络科技有限公司、六安校无忧信息科技有限公司、辽宁路为物流有限公司、理光（中国）投资有限公司、廊坊市极致网络科技有限公司、酷渲（北京）科技有限公司、酷溜网（北京）文化传媒有限公司、江西铭软科技有限公司、济南速动信息科技有限公司、湖南强智科技发展有限公司、湖南翱云网络科技有限公司、洪湖尔创网联信息技术有限公司、黑龙江立高科技股份有限公司、合肥奇乐网络科技有限公司、杭州融都科技股份有限公司、杭州可道云网络有限公司、杭州海康威视数字技术股份有限公司、海南赞赞网络科技有限公司、国泰君安证券股份有限公司、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、广州同鑫科技有限公司、广州龙建达电子股份有限公司、广联达科技股份有限公司、广东拓迪智能科技有限公司、富士施乐（中国）有限

公司、创维集团有限公司、成都依能科技股份有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、北京中庆纳博信息技术有限公司、北京智慧远景科技产业有限公司、北京智邦国际软件技术有限公司、北京星网锐捷网络技术有限公司、北京万维盈创科技发展有限公司、北京硕人时代科技股份有限公司、北京数科网维技术有限责任公司、北京恰维网络科技有限公司、北京金和网络股份有限公司、北京棣南新宇科技有限公司、北京百卓网络技术有限公司、北尔电子贸易（上海）有限公司、爱普生（中国）有限公司、Axis 网络通讯有限公司、阿里巴巴集团安全应急响应中心、腾讯安全应急响应中心、联想集团、上海程江科技中心、信呼、梦想 CMS、剑鱼论坛、广安日报社、港华燃气集团、帝国软件、爱青檬 CMS、OPPO 安全应急响应中心、TaoLer 社区系统、YZNCMS、YimaoAdmin、Textpattern CMS、SparkPost、SEMCMS、seacms、Rockwell Automation、PHPCMS、Oracle、MuYuCMS、JrkAdmin、hadsky、dwz-hinkphp323、AKCMS、A3MALL 和 Wuhan Deepin Technology Co.。

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、北京华顺信安科技有限公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、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。山东云天安全技术有限公司、北京山石网科信息技术有限公司、北京信联科汇科技有限公司、杭州木链物联网科技有限公司、江西省掌控者信息安全技术有限公司、南京众智维信息科技有限公司、上海纽盾科技股份有限公司、河南灵创电子科技有限公司、杭州迪普科技股份有限公司、北京天地和兴科技有限公司、河南信安世纪科技有限公司、重庆都会信息科技有限公司、广东蓝爵网络安全技术股份有限公司、安徽长泰信息安全服务有限公司、河南东方云盾信息技术有限公司、北京安帝科技有限公司、北京升鑫网络科技有限公司、北京远禾科技有限公司、北京网御星云信息技术有限公司、武汉明嘉信信息安全检测评估有限公司、广州易东信息安全技术有限公司、北京顶象技术有限公司、山东新潮信息技术有限公司、浙江御安信息技术有限公司、京东云安全、南京树安信息技术有限公司、亚信科技（成都）有限公司、浙江大学控制科学与工程学院、北京机沃科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、贵州多彩宝互联网服务有限公司、江苏省信息安全测评中心、清远职业技术学院、上海市信息安全测评认证中心、山东泽鹿安全技术有限公司、浙江菜鸟供应链管理有限公司、中国工商银行、中油国际管道公司及其他个人白帽子向 CNVD 提交了 4147 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 1849 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）	728	728
奇安信网神（补天平台）	658	658
北京天融信网络安全技术有限公司	602	2
上海交大	463	463
北京华顺信安科技有限公司	310	1
哈尔滨安天科技集团股份有限公司	260	0
华为技术有限公司	213	0
新华三技术有限公司	164	0
恒安嘉新（北京）科技股份公司	129	0
北京数字观星科技有限公司	114	0
北京神州绿盟科技有限公司	84	12
北京启明星辰信息安全技术有限公司	60	2
天津市国瑞数码安全系统股份有限公司	59	0
北京奇虎科技有限公司	55	10
深信服科技股份有限	40	0

公司		
北京知道创宇信息技术股份有限公司	25	20
远江盛邦（北京）网络安全科技股份有限公司	12	12
南京联成科技发展股份有限公司	11	11
北京长亭科技有限公司	8	8
卫士通信息产业股份有限公司	6	0
北京安信天行科技有限公司	5	5
南京铱迅信息技术股份有限公司	1	1
山东云天安全技术有限公司	328	328
北京山石网科信息技术有限公司	251	251
北京信联科汇科技有限公司	195	195
杭州木链物联网科技有限公司	119	119
联想集团	82	0
江西省掌控者信息安全技术有限公司	73	73
西门子（中国）有限公司	66	0
南京众智维信息科技有限公司	58	58
上海纽盾科技股份有限公司	29	29
河南灵创电子科技有	27	27

限公司		
中国电信股份有限公司网络安全产品运营中心	20	0
杭州迪普科技股份有限公司	19	5
北京天地和兴科技有限公司	18	18
河南信安世纪科技有限公司	18	18
重庆都会信息科技有限公司	14	14
广东蓝爵网络安全技术股份有限公司	13	13
安徽长泰信息安全服务有限公司	12	12
河南东方云盾信息技术有限公司	10	10
北京安帝科技有限公司	8	8
北京升鑫网络科技有限公司	7	7
北京远禾科技有限公司	7	7
北京网御星云信息技术有限公司	6	6
武汉明嘉信信息安全检测评估有限公司	6	6
广州易东信息安全技术有限公司	5	5
北京顶象技术有限公司	4	4
山东新潮信息技术有限公司	4	4

浙江御安信息技术有限公司	4	4
京东云安全	3	3
南京树安信息技术有限公司	3	3
亚信科技（成都）有限公司	3	3
浙江大学控制科学与工程学院	3	3
北京机沃科技有限公司	2	2
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
贵州多彩宝互联网服务有限公司	1	1
江苏省信息安全测评中心	1	1
清远职业技术学院	1	1
上海市信息安全测评认证中心	1	1
山东泽鹿安全技术有限公司	1	1
浙江菜鸟供应链管理有限公司	1	1
中国工商银行	1	1
中油国际管道公司	1	1
CNCERT 青海分中心	15	15
CNCERT 宁夏分中心	1	1
CNCERT 山东分中心	1	1
个人	952	952
报送总计	6403	4147

本周漏洞按类型和厂商统计

本周，CNVD 收录了 575 个漏洞。WEB 应用 269 个，应用程序 172 个，网络设备（交换机、路由器等网络端设备）57 个，操作系统 35 个，智能设备（物联网终端设备）22 个，安全产品 20 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	269
应用程序	172
网络设备（交换机、路由器等网络端设备）	57
操作系统	35
智能设备（物联网终端设备）漏洞	22
安全产品	20

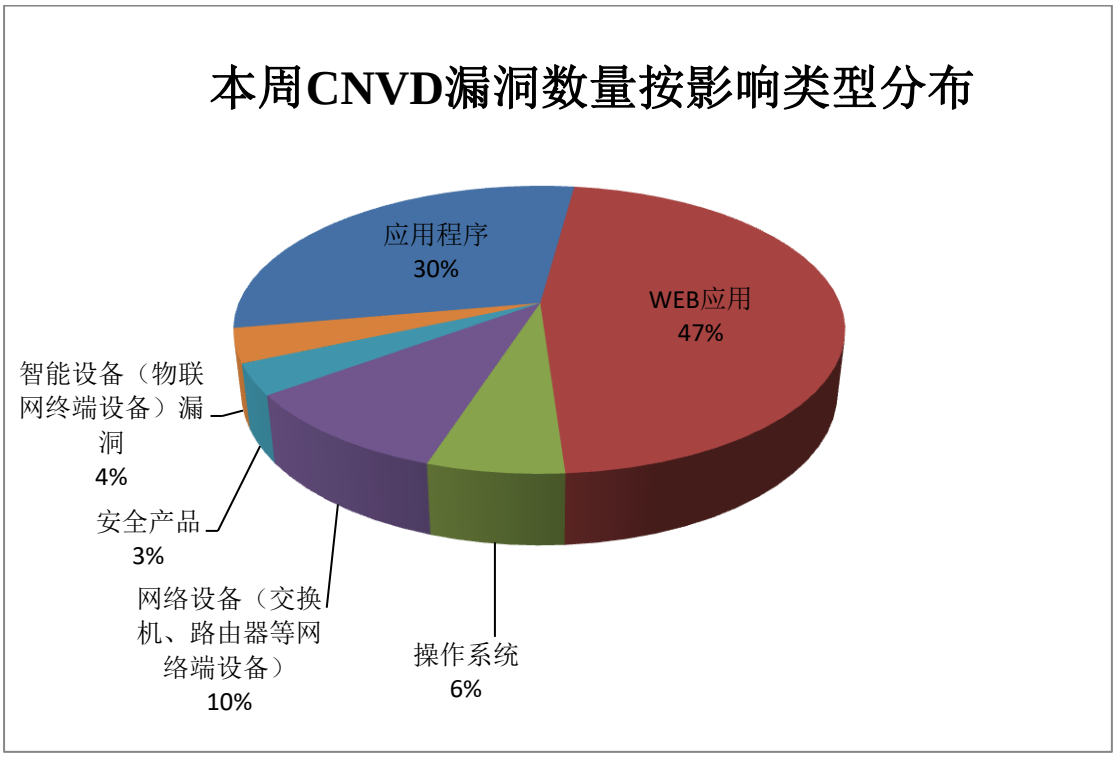

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及爱青檬 CMS、Siemens、Cisco 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	爱青檬 CMS	41	7%
2	Siemens	31	5%
3	Cisco	15	3%
4	NETGEAR	15	3%
5	MicroTik	14	2%

6	北京棣南新宇科技有限公司	14	2%
7	Adobe	11	2%
8	Aruba	10	2%
9	IBM	10	2%
10	其他	414	72%

本周行业漏洞收录情况

本周，CNVD 收录了 59 个电信行业漏洞，17 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Siemens RUGGEDCOM ROS Devices 缓冲区溢出漏洞、D-Link DAP-1330 缓冲区溢出漏洞、Cisco IOS XE 快速重载漏洞、多款 NETGEAR 产品命令注入漏洞（CNVD-2021-50928）”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/

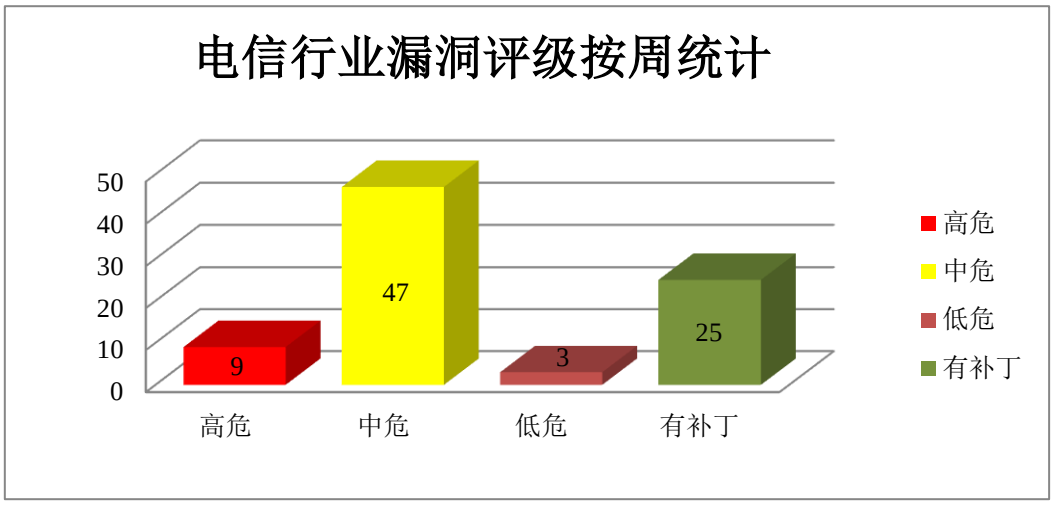

图 3 电信行业漏洞统计

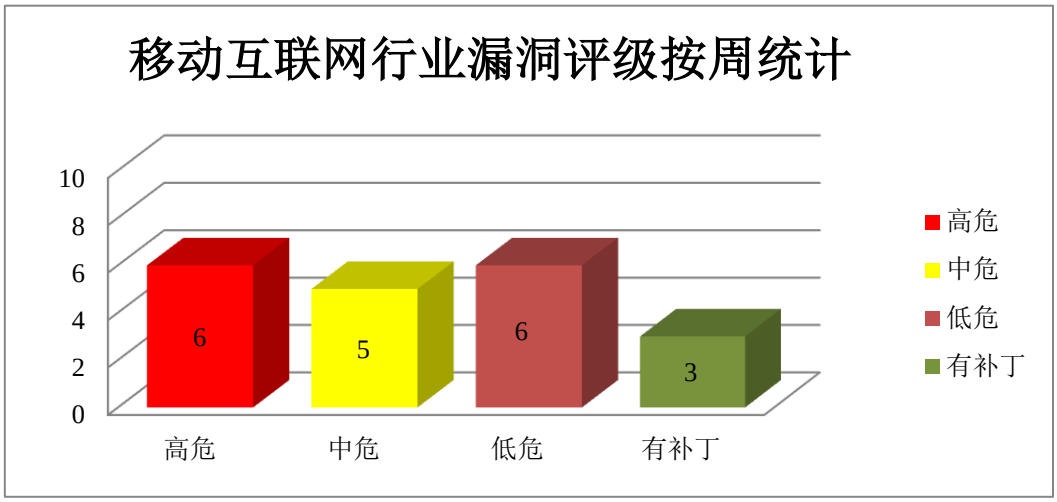

图 4 移动互联网行业漏洞统计

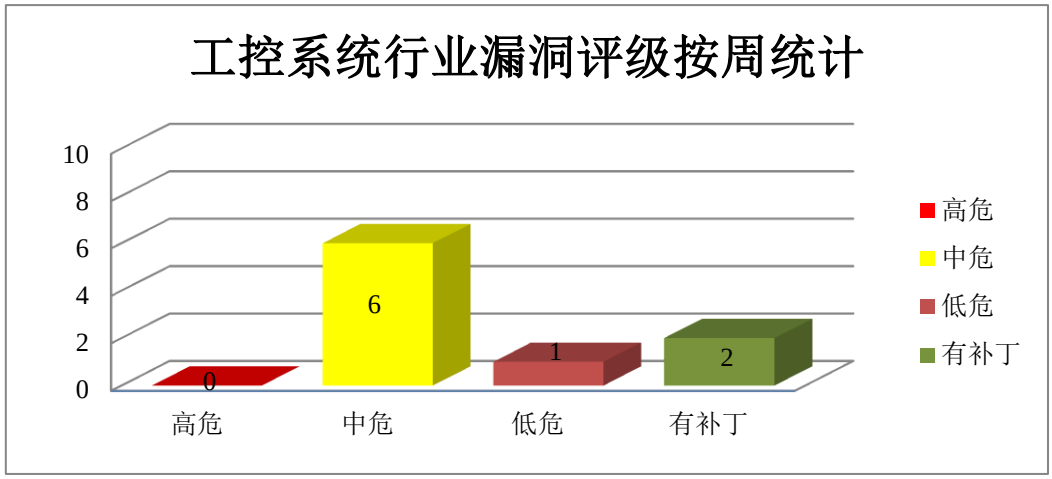

图 5 工控系统行业漏洞统计

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 Media Encoder 是一款视频和音频编码应用程序。Adobe Animate 是一款多媒体创作和计算机动画程序。Medium by Adobe 是一款 VR 艺术创作工具。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，提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Media Encoder 越界读取漏洞（CNVD-2021-49602）、Adobe Animate 释放后重用漏洞、Adobe Animate 越界写入漏洞（CNVD-2021-49604）、Adobe Medium 输入验证错误漏洞、Adobe Animate 越界读取漏洞（CNVD-2021-49606、CNVD-2021-49609、CNVD-2021-49608、CNVD-2021-49607）。其中，“Adobe Media Encoder 越界读取漏洞（CNVD-2021-49602）、Adobe Animate 释放后重用漏

洞、Adobe Animate 越界写入漏洞（CNVD-2021-49604）、Adobe Medium 输入验证错误漏洞”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-2021-49602

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49606

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49605

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49604

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49603

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49609

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49608

https://www.cnvd.org.cn/flaw/show/CNVD-2021-49607

2、Cisco 产品安全漏洞

Cisco IOS XE 是美国 Cisco 公司为其网络设备开发的一套基于 Linux 内核的模块化操作系统。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 是一个网络设备。用于保护各种规模的公司网络和数据中心。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以 root 权限在底层操作系统上执行命令，执行未签名的二进制文件，导致进程崩溃等。

CNVD 收录的相关漏洞包括：Cisco Firepower Threat Defense 命令注入漏洞、Cisco Firepower Threat Defense 拒绝服务漏洞（CNVD-2021-50578）、Cisco IOS XE 快速重载漏洞（CNVD-2021-50584、CNVD-2021-50585）、Cisco Adaptive Security Appliance 和 Firepower Threat Defense 命令注入漏洞、Cisco Adaptive Security Appliance 和 Firepower Threat Defense 拒绝服务漏洞（CNVD-2021-50581、CNVD-2021-50582）、Cisco IOS 和 IOS XE 权限提升漏洞。其中，除“Cisco Adaptive Security Appliance 和 Firepower Threat Defense 拒绝服务漏洞（CNVD-2021-50581）”外的综合评级为“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-2021-50579

https://www.cnvd.org.cn/flaw/show/CNVD-2021-50578

https://www.cnvd.org.cn/flaw/show/CNVD-2021-50584

https://www.cnvd.org.cn/flaw/show/CNVD-2021-50583

https://www.cnvd.org.cn/flaw/show/CNVD-2021-50582

https://www.cnvd.org.cn/flaw/show/CNVD-2021-50581

https://www.cnvd.org.cn/flaw/show/CNVD-2021-50587

https://www.cnvd.org.cn/flaw/show/CNVD-2021-50585

3、NETGEAR 产品安全漏洞

NETGEAR WAC505 是美国网件（NETGEAR）公司的一款无线接入点（AP）。NETGEAR EX7000 是一款无线网络信号扩展器。NETGEAR R8500 是一款无线路由器。NETGEAR R6250 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR R8300 是一款无线路由器。NETGEAR D6400 是一款无线调制解调器。NETGEAR D6220 是一款无线调制解调器。NETGEAR D7800 是一款无线调制解调器。NETGEAR R7500 是一款无线路由器。NETGEAR WNDR3700 是一款无线路由器。NETGEAR R6700 是一款无线路由器。NETGEAR R7900 是一款无线路由器。NETGEAR EX3700 是一款无线网络信号扩展器。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受影响客户端向服务器发送非预期的请求，绕过身份验证，执行非法操作系统命令，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品跨站请求伪造漏洞（CNVD-2021-50917）、多款 NETGEAR 产品授权问题漏洞（CNVD-2021-50922、CNVD-2021-50918）、多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-50921、CNVD-2021-50925、CNVD-2021-50924、CNVD-2021-50926）、多款 NETGEAR 产品命令注入漏洞（CNVD-2021-50928）。其中，“多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-50925、CNVD-2021-50924）、多款 NETGEAR 产品命令注入漏洞（CNVD-2021-50928）”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-2021-50918
https://www.cnvd.org.cn/flaw/show/CNVD-2021-50917
https://www.cnvd.org.cn/flaw/show/CNVD-2021-50922
https://www.cnvd.org.cn/flaw/show/CNVD-2021-50921
https://www.cnvd.org.cn/flaw/show/CNVD-2021-50925
https://www.cnvd.org.cn/flaw/show/CNVD-2021-50924
https://www.cnvd.org.cn/flaw/show/CNVD-2021-50928
https://www.cnvd.org.cn/flaw/show/CNVD-2021-50926

4、Siemens 产品安全漏洞

Siemens SINAMICS SL150 是德国西门子（Siemens）公司的一个应用程序。用于高转矩慢速同步和感应电动机的循环变频器。Siemens RuggedCom ROS 是一套用于 RuggedCom 系列交换机中的操作系统。Siemens Jt2go 是一款 JT 文件查看器。Siemens Teamcenter Visualization 是一个可为设计 2D、3D 场景提供团队协作功能的软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未经过身份验证的远程访问引起拒绝服务条件，或执行有限的配置修改，或执行有限的控制命令，在当前进程的上下文中执行代码等。

CNVD 收录的相关漏洞包括：Siemens SINAMICS SL150 输入验证错误漏洞、Sie

mens RUGGEDCOM ROS Devices 缓冲区溢出漏洞、Siemens JT2Go 和 Teamcenter Visualization 堆缓冲区溢出漏洞（CNVD-2021-51449、CNVD-2021-51450）、Siemens JT2Go 和 Teamcenter Visualization 越界写入漏洞（CNVD-2021-51448、CNVD-2021-51456、CNVD-2021-51451）、Siemens JT2Go 和 Teamcenter Visualization 越界读取漏洞（CNVD-2021-51452）。其中，“Siemens SINAMICS SL150 输入验证错误漏洞、Siemens RUGGEDCOM ROS Devices 缓冲区溢出漏洞”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-2021-51323
https://www.cnvd.org.cn/flaw/show/CNVD-2021-51441
https://www.cnvd.org.cn/flaw/show/CNVD-2021-51449
https://www.cnvd.org.cn/flaw/show/CNVD-2021-51448
https://www.cnvd.org.cn/flaw/show/CNVD-2021-51452
https://www.cnvd.org.cn/flaw/show/CNVD-2021-51451
https://www.cnvd.org.cn/flaw/show/CNVD-2021-51450
https://www.cnvd.org.cn/flaw/show/CNVD-2021-51456

5、MikroTik RouterOS 内存破坏漏洞（CNVD-2021-49784）

MikroTik RouterOS 是拉脱维亚 MikroTik 公司的一套基于 Linux 开发的路由器操作系统。该系统可部署在 PC 中，使其提供路由器功能。本周，MikroTik RouterOS 被披露存在内存破坏漏洞。攻击者可利用该漏洞导致拒绝服务。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-2021-49784

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-2021-50091	Aruba ClearPass Policy Manager 命令执行漏洞（CNVD-2021-50091）	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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-012.txt
CNVD-2021-50138	多款 Texas Instruments 产品整数溢出或环绕漏洞（CNVD-2021-50138）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ti.com/technologies/security/report-product-security-vulnerabilities.html
CNVD-2021-	WordPress 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏

50143	（CNVD-2021-50143）		洞，补丁获取链接：https://wpscan.com/vulnerability/eec0f29f-a985-4285-8eed-d1855d204a20
CNVD-2021-50153	RebornCore library 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/TechReborn/RebornCore/security/advisories/GHSA-r7pg-4xrf-7mrm
CNVD-2021-50165	Fortinet FortiMail 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.fortiguard.com/psirt/FG-IR-21-027
CNVD-2021-50178	IBM Guardium Data Encryption 信息泄露漏洞	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.ibm.com/blogs/psirt/security-bulletin-vulnerability-in-ibm-guardium-data-encryption-gde-cve-2021-20414/
CNVD-2021-50184	PbootCMS 远程代码执行漏洞	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.pbootcms.com/changelog/
CNVD-2021-51435	Samsung Tizen 代码注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.samsungmobile.com/serviceWeb.smsb?year=2021&month=7
CNVD-2021-51474	D-Link DAP-1330 缓冲区溢出漏洞	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.zerodayinitiative.com/advisories/ZDI-21-681/
CNVD-2021-51483	Microsoft Exchange Server 远程代码执行漏洞（CNVD-2021-51483）	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-2021-31206

小结：本周，Adobe 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，提升权限，执行任意代码等。此外，Cisco、NETGEAR、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过受影响客户端向服务器发送非预期的请求，绕过身份验证，以 root 权限在底层操作系统上执行命令，执行未签名的二进制文件，导致进程崩溃或缓冲区溢出或堆溢出等。另外，MikroTik RouterOS 被披露存在内存破坏漏洞。攻击者可利用该漏洞导致拒绝服务。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、Halo 服务器端请求伪造漏洞

验证描述

Halo 是一款轻快、简洁的 Java 博客系统。

Halo 1.3.2 及更早版本中的 SMTP 配置存在服务器端请求伪造漏洞，攻击者可利用该漏洞检测服务器内网。

验证信息

POC 链接：https://github.com/halo-dev/halo/issues/806

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-50934

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. CDN 服务商 Cloudflare 的 cdnjs 库发现远程代码执行漏洞

CDN 服务商 Cloudflare 的 JavaScript/CSS 库 cdnjs 发现了一个远程代码执行漏洞。cdnjs 是最广泛使用的 JS 库之一，利用 cdnjs 的漏洞发动供应链攻击将会影响无数的网站。

参考链接：https://www.solidot.org/story?sid=68303

2. 谷歌：四个 0day 漏洞被积极利用，领英已被攻击

谷歌安全人员分享了 4 个新的 0day 漏洞的信息。并且，谷歌还透露，与俄罗斯有关的 APT 组织正在利用其中的 Safari 零日漏洞攻击 LinkedIn 用户。

参考链接：https://www.freebuf.com/news/280870.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