

信息安全漏洞周报

2021 年 10 月 18 日-2021 年 10 月 24 日

2021 年第 42 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 402 个，其中高危漏洞 117 个、中危漏洞 231 个、低危漏洞 54 个。漏洞平均分为 5.63。本周收录的漏洞中，涉及 0day 漏洞 334 个（占 83%），其中互联网上出现“libde265 堆缓冲区溢出漏洞（CNVD-2021-78426）、libde265 堆缓冲区溢出漏洞（CNVD-2021-78427）”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原创漏洞总数 7662 个，与上周（5750 个）环比增加 33%。

CNVD收录漏洞近10周平均分分布图

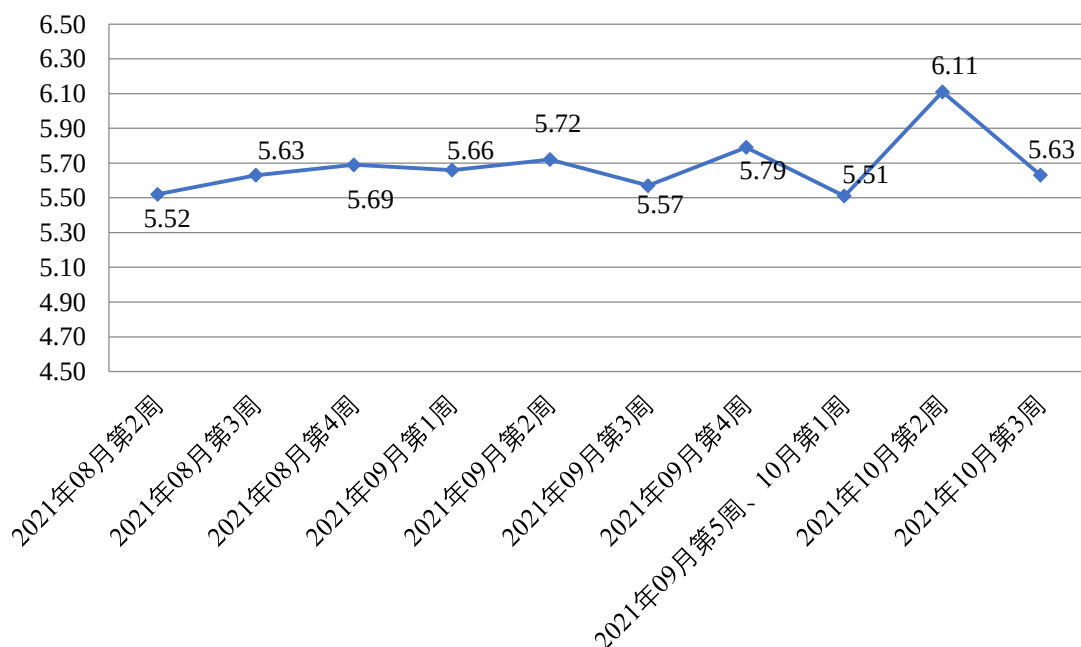


图 1 CNVD 收录漏洞近 10 周平均分分布图



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 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 709 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 79 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 95 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：

紫光软件系统有限公司、淄博闪灵网络科技有限公司、中兴通讯股份有限公司、浙江和达科技股份有限公司、浙江大华技术股份有限公司、长沙市轨道交通集团有限公司、长江勘测规划设计研究有限责任公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、新开普电子股份有限公司、新华三技术有限公司、小米科技有限责任公司、西门子（中国）有限公司、武汉斗鱼网络科技有限公司、微宏软件技术(杭州)有限公司、苏州万户网络科技有限公司、松下电器（中国）有限公司、四创科技有限公司、四川湖山电器股份有限公司、神州数码集团股份有限公司、深圳英飞拓科技股份有限公司、深圳市中瑞奇电子科技有限公司、深圳市中科网威科技有限公司、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、深圳市分寸科技有限公司、上海卓卓网络科技有限公司、上海新网程信息技术股份有限公司、上海商创网络科技有限公司、上海任意门科技有限公司、上海勤和互联网技术软件开发有限公司、上海安达通信息安全技术股份有限公司、熵基科技股份有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、普联技术有限公司、宁波江北希品网络科技有限公司、南京汇微达信息技术有限公司、茉柏桢（上海）软件科技有限公司、洛阳云业信息科技有限公司、龙采科技集团有限责任公司、联通数字科技有限公司、理光（中国）投资有限公司、江西铭软科技有限公司、江苏群立现代信息科技发展有限公司、建荣皇家海洋科普世界（沈阳）有限公司、佳能（中国）有限公司、济南卓源软件有限公司、华为技术有限公司、河南礼恰网络科技有限公司、河北鑫考教育科技股份有限公司、河北南昊高新技术开发有限公司、航天信息股份有限公司、杭州雄伟科技开发股份有限公司、杭州三汇信息工程有限公司、杭州恩软信息技术有限公司、杭州短趣网络传媒技术有限公司、杭州贝腾科技有限公司、海尔集团电子商务有限公司、广州市奥威亚电子科技有限公司、广州好象科技有限公司、广东泰恪网络科技有限公司、福建四创软件有限公司、飞救医疗科技（北京）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、北京中科网威信息技术有限公司、北京致远互联软件股份有限公司、北京星网锐捷网络技术有限公司、北京沃丰时代数据科技有限公司、北京网御星云信息技术有限公司、北京通达信科科技有限公司、北京山石网科信息技术有限公司、北京三快科技有限公司、北京融智合

创科技有限公司、北京汉邦高科数字技术股份有限公司、北京创世新强科技有限公司、海联集团、中国卫星导航定位协会、中国农业机械化科学研究院、奥壹科技（OE）团队、梦想 CMS、ZZCMS、yycms、XnSoft、Trendnet、The Apache Software Foundation、Teledyne FLIR、taoCMS、SoftMaker、SEMCMS、Lexmark、Joomla、HDHCMS、Hancorn 和 Best IT World(India) Pvt. Ltd。

本周，CNVD 发布了《Oracle 发布 2021 年 10 月的安全公告》。详情参见 CNVD 网站公告内容。

<https://www.cnvd.org.cn/webinfo/show/6941>

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京数字观星科技有限公司、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、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、河南灵创电子科技有限公司、北京华云安信息技术有限公司、北京信联科汇科技有限公司、南京众智维信息科技有限公司、杭州迪普科技股份有限公司、京东云安全、CNVD 众测平台、北京安帝科技有限公司、安徽长泰科技有限公司、杭州海康威视数字技术股份有限公司、山东新潮信息技术有限公司、新疆海狼科技有限公司、北京惠而特科技有限公司、内蒙古洞明科技有限公司、重庆都会信息科技、浙江木链物联网科技有限公司、江苏快页信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、长春嘉诚信息技术股份有限公司、平安银河实验室、内蒙古云科数据服务股份有限公司、云南南天电子信息产业股份有限公司、河南信安世纪科技有限公司、广州安亿信软件科技有限公司、思而听网络科技有限公司、南京树安信息技术有限公司、百度 AIoT 安全团队、山东泽鹿安全技术有限公司、陕西省网络与信息安全测评中心、武汉绿色网络信息服务有限责任公司、银保信科技（北京）有限公司、北京机沃科技有限公司、华润（集团）有限公司、山石网科通信技术股份有限公司、北京远禾科技有限公司、北京网御星云信息技术有限公司、中国银行、福建省海峡信息技术有限公司、北京威努特技术有限公司及其他个人白帽子向 CNVD 提交了 7662 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 5696 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)	4516	4516
上海交大	664	664
奇安信网神（补天平台）	516	516

北京数字观星科技有限公司	461	0
北京神州绿盟科技有限公司	375	15
哈尔滨安天科技集团股份有限公司	254	0
华为技术有限公司	203	0
新华三技术有限公司	110	0
北京奇虎科技有限公司	100	0
深信服科技股份有限公司	97	0
恒安嘉新（北京）科技股份有限公司	90	0
北京启明星辰信息安全技术有限公司	63	5
天津市国瑞数码安全系统股份有限公司	59	0
远江盛邦（北京）网络安全科技股份有限公司	33	33
南京联成科技发展股份有限公司	28	28
西安四叶草信息技术有限公司	18	18
北京天融信网络安全技术有限公司	9	9
北京知道创宇信息技术有限公司	5	5
卫士通信息产业股份有限公司	3	0
杭州安恒信息技术股份有限公司	2	2
内蒙古奥创科技有限公司	2	2
联想集团	299	0
山东云天安全技术有限公司	126	126
河南灵创电子科技有限公司	107	107
北京华云安信息技术有限公司	95	95
北京信联科汇科技有	85	85

限公司		
南京众智维信息科技有限公司	79	79
杭州迪普科技股份有限公司	77	77
中国电信股份有限公司网络安全产品运营中心	60	0
京东云安全	50	50
CNVD 众测平台	47	47
北京安帝科技有限公司	43	43
安徽长泰科技有限公司	41	41
杭州海康威视数字技术股份有限公司	40	40
山东新潮信息技术有限公司	29	29
亚信科技（成都）有限公司	27	0
新疆海狼科技有限公司	23	23
北京惠而特科技有限公司	17	17
内蒙古洞明科技有限公司	16	16
重庆都会信息科技	11	11
浙江木链物联网科技有限公司	11	11
江苏快页信息技术有限公司	9	9
北京云科安信科技有限公司（Seraph 安全实验室）	8	8
长春嘉诚信息技术股份有限公司	6	6
平安银河实验室	4	4
内蒙古云科数据服务股份有限公司	4	4
云南南天电子信息产业股份有限公司	3	3
河南信安世纪科技有限公司	3	3

广州安亿信软件科技有限公司	3	3
思而听网络科技有限公司	3	3
南京树安信息技术有限公司	2	2
百度 AIoT 安全团队	2	2
山东泽鹿安全技术有限公司	2	2
陕西省网络与信息安全测评中心	2	2
武汉绿色网络信息服务有限责任公司	1	1
银保信科技（北京）有限公司	1	1
北京机沃科技有限公司	1	1
华润（集团）有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京远禾科技有限公司	1	1
北京网御星云信息技术有限公司	1	1
中国银行	1	1
福建省海峡信息技术有限公司	1	1
北京威努特技术有限公司	1	1
CNCERT 宁夏分中心	15	15
CNCERT 贵州分中心	6	6
CNCERT 四川分中心	5	5
个人	865	865
报送总计	9843	7662

本周漏洞按类型和厂商统计

本周，CNVD 收录了 402 个漏洞。WEB 应用 165 个，应用程序 113 个，网络设备（交换机、路由器等网络端设备）67 个，智能设备（物联网终端设备）40 个，操作系统 12 个，安全产品 3 个，数据库 2 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	165
应用程序	113
网络设备（交换机、路由器等网络端设备）	67
智能设备（物联网终端设备）	40
操作系统	12
安全产品	3
数据库	2

本周CNVD漏洞数量按影响类型分布

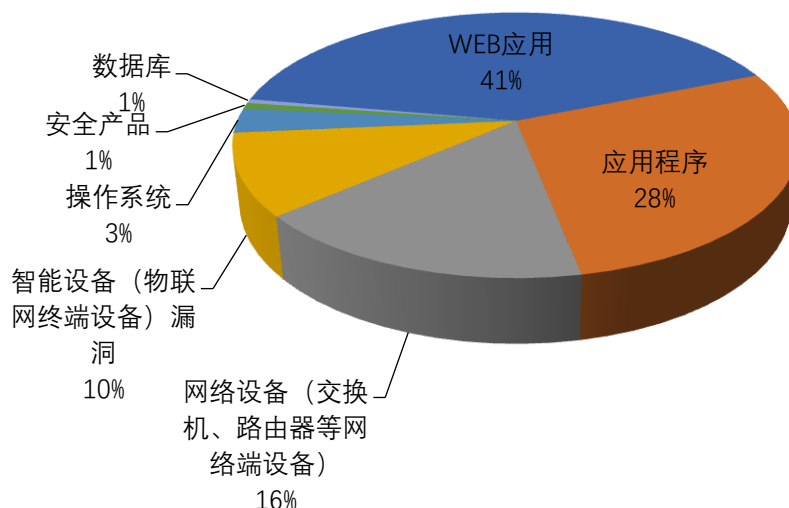


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及新华三技术有限公司、ZOHO、Mozilla 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	新华三技术有限公司	38	9%
2	ZOHO	17	4%
3	Mozilla	13	3%
4	Cybozu	13	3%
5	Google	12	3%
6	Lexmark International Inc	11	2%
7	libde265	9	2%
8	Lexmark	9	2%
9	IBM	8	2%
10	其他	272	70%

本周行业漏洞收录情况

本周，CNVD 收录了 61 个电信行业漏洞，19 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“Google Android WideVine 代码执行漏洞、Google Android MessageQueueBase.h 缓冲区溢出漏洞”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/>

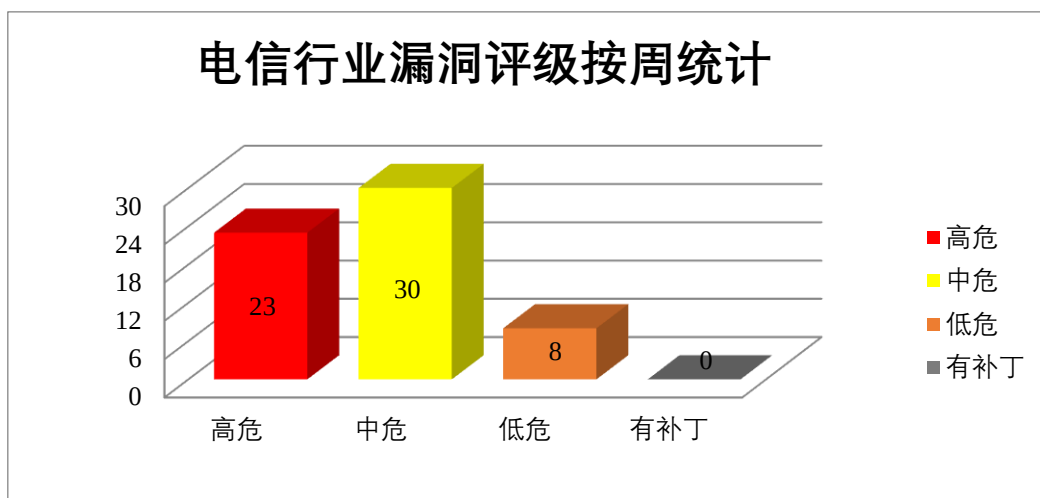


图 3 电信行业漏洞统计

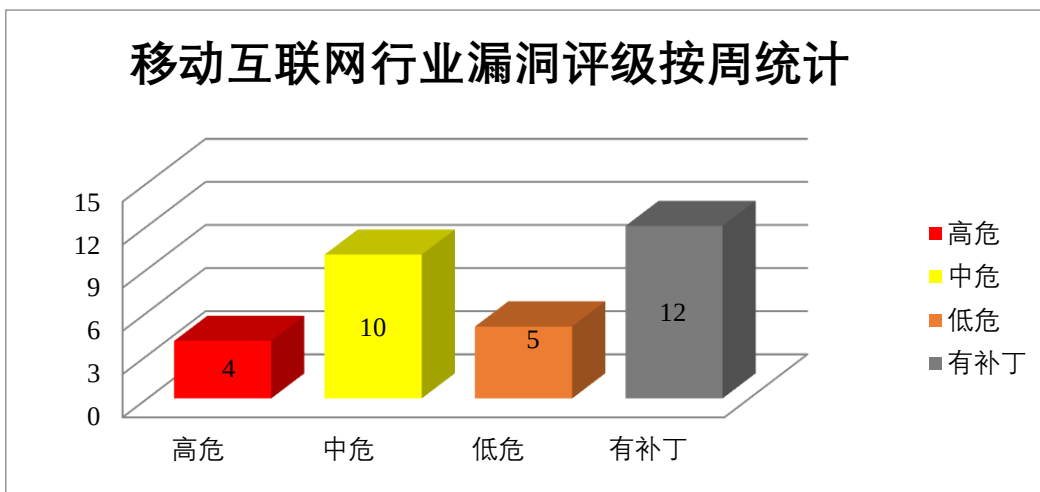


图 4 移动互联网行业漏洞统计

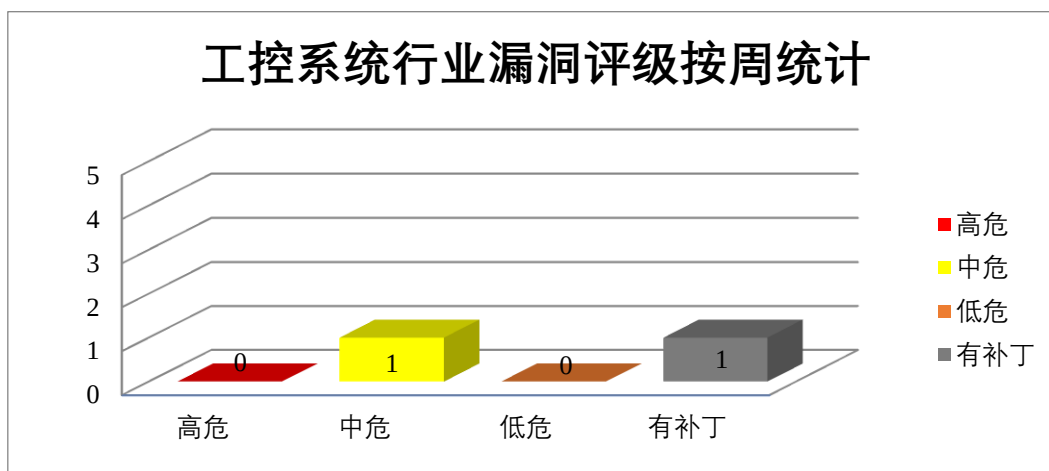


图 5 工控系统行业漏洞统计

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、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，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2021-78770、CNVD-2021-78773、CNVD-2021-78772、CNVD-2021-78771、CNVD-2021-78776、CNVD-2021-78775）、Google Android MessageQueueBase.h 缓冲区溢出漏洞、Google Android WideVine 代码执行漏洞。其中，“Google Android MessageQueueBase.h 缓冲区溢出漏洞、Google Android WideVine 代码执行漏洞”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-2021-78770>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78773>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78772>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78771>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78776>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78775>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78781>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78780>

2、ZOH0 产品安全漏洞

ZOH0 ManageEngine ADManager Plus 是美国卓豪（ZOH0）公司的一套为使用 W

indows 域的企业用户设计的微软活动目录管理软件。该软件能够协助 AD 管理员和帮助台技术人员进行日常管理工作，例如批量管理用户帐户和 AD 对象、给帮助台技术员指派基于角色的访问权限等。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致远程代码执行。

CNVD 收录的相关漏洞包括：ZOHO ManageEngine ADManager Plus 文件上传漏洞（CNVD-2021-78727、CNVD-2021-78730、CNVD-2021-78729、CNVD-2021-78728、CNVD-2021-78733、CNVD-2021-78732、CNVD-2021-78731、CNVD-2021-78736）。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-2021-78727>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78730>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78729>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78728>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78733>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78732>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78731>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78736>

3、Mozilla 产品安全漏洞

Rust 是 Mozilla 基金会的一款通用、编译型编程语言。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致内存损坏、数据竞争和未定义的行为等。

CNVD 收录的相关漏洞包括：Mozilla Rust 命令注入漏洞（CNVD-2021-78744、CNVD-2021-78750）、Mozilla Rust 内存破坏漏洞（CNVD-2021-78747）、Mozilla Rust 内存泄露漏洞、Mozilla Rust 缓冲区溢出漏洞（CNVD-2021-78756、CNVD-2021-78755、CNVD-2021-78754、CNVD-2021-78753）。其中，“Mozilla Rust 内存破坏漏洞（CNVD-2021-78747）、Mozilla Rust 内存泄露漏洞”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-2021-78744>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78747>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78750>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78754>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78753>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78752>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78756>
<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78755>

4、IBM 产品安全漏洞

IBM Sterling File Gateway 是一款用于在内部和外部合作伙伴之间传输文件的应用程序，可让您更加安全可靠地与贸易伙伴进行文件传输。IBM Sterling B2B Integrator 是一个交易引擎，是一套根据您的业务需求运行您定义和管理的流程的组件。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敏感信息、上传任意文件等。

CNVD 收录的相关漏洞包括：IBM Sterling File Gateway 跨站请求伪造漏洞、IBM Sterling File Gateway 跨站脚本漏洞（CNVD-2021-78435、CNVD-2021-78438）、IBM Sterling File Gateway 信息泄露漏洞（CNVD-2021-78437、CNVD-2021-78442、CNVD-2021-78441）、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2021-78440）、IBM Sterling File Gateway 任意文件上传漏洞。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-2021-78436>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78435>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78438>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78437>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78440>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78439>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78442>

<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78441>

5、Mozilla Rust 内存破坏漏洞（CNVD-2021-78745）

Rust 是 Mozilla 基金会的一款通用、编译型编程语言。本周，Mozilla Rust 被披露存在内存破坏漏洞。攻击者可利用该漏洞导致未定义的行为，如数据竞争。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-2021-78745>

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-2021-78735	ZOHO ManageEngine ADManager Plus 文件上传漏洞（CNVD-2021-78735）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.manageengine.com/products/ad-manager/release-notes.html#7111
CNVD-2021-78734	ZOHO ManageEngine ADManager Plus 文件上传漏洞（CNVD-2021-78734）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.manageengine.com/prod

			ucts/ad-manager/release-notes.html#7111
CNVD-2021-78739	ZOHO ManageEngine ADSelfService Plus SQL 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://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6112-hotfix-release
CNVD-2021-78738	ZOHO ManageEngine ADManager Plus 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.manageengine.com/products/ad-manager/release-notes.html#7111
CNVD-2021-78737	ZOHO ManageEngine ADManager Plus 文件上传漏洞（CNVD-2021-78737）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.manageengine.com/products/ad-manager/release-notes.html#7111
CNVD-2021-78742	ZOHO ManageEngine ADSelfService Plus CSV 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.manageengine.jp/

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码等。此外，ZOHO、Mozilla、IBM 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、上传任意文件、导致内存损坏、远程代码执行等。另外，Rust 被披露存在内存破坏漏洞。攻击者可利用该漏洞导致未定义的行为，如数据竞争。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、libde265 堆缓冲区溢出漏洞（CNVD-2021-78427）

验证描述

libde265 是 h.265 视频编解码器的开源实现。

libde265 1.0.4 版中的 mc_luma 函数存在堆缓冲区溢出漏洞，攻击者可通过特制文件利用该漏洞导致拒绝服务。

验证信息

POC 链接：<https://github.com/strukturag/libde265/issues/239>

参考链接：<https://www.cnvd.org.cn/flaw/show/CNVD-2021-78427>

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. 微软发布针对老款设备——Surface Pro 3 新漏洞的安全警告

攻击者可利用该漏洞破坏设备认证机制，将恶意设备引入企业网络中。

参考链接：<https://www.freebuf.com/news/292423.html>

2. WinRAR 惊现远程代码执行漏洞

网络安全专家 Igor Sak-Sakovskiy 发现了 WinRAR 的一个远程代码执行漏洞，漏洞编号 CVE-2021-35052。该漏洞出现在 WinRAR 的 Windows 试用版本，漏洞版本为 5.70，黑客可利用该漏洞远程攻击计算机系统。

参考链接：<https://securityaffairs.co/wordpress/123652/hacking/winrar-trial-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