国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 09 月 14 日-2020 年 09 月 20 日　　2020 年第 38 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 395 个，其中高危漏洞 94 个、中危漏洞 231 个、低危漏洞 70 个。漏洞平均分值为 5.43。本周收录的漏洞中，涉及 0day 漏洞 51 个（占 13%），其中互联网上出现“Linux expand_downwards()竞争条件漏洞、Open Solutions for Education openSIS SQL 注入漏洞（CNVD-2020-52193）”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 2152 个，与上周（4632 个）环比增加 54%。

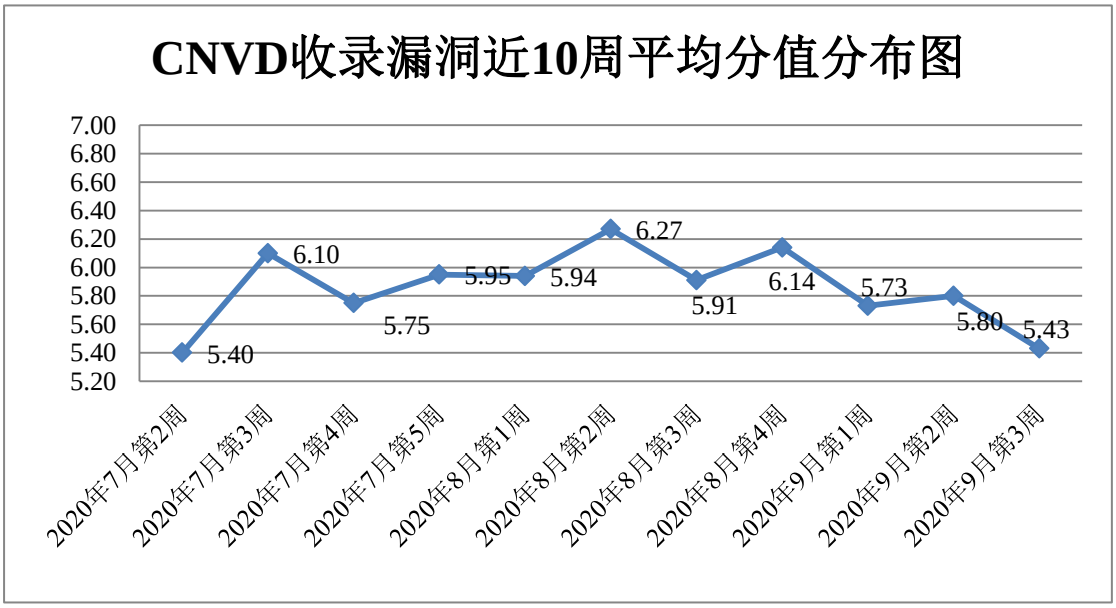

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 起，向基础电信企业通报漏洞事件 11 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 239 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 54 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 24 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：

珠海金山办公软件有限公司、上海黄豆网络科技有限公司、深圳市富士智能系统有限公司、北京天融信科技有限公司、厦门四信通信科技有限公司、中移铁通有限公司智能产品分公司、深圳市惟新控股有限合伙企业、深圳市迅雷网文化有限公司、深圳维盟科技股份有限公司、瑞芯微电子股份有限公司、南京裕后网络科技有限公司、北京汉邦高科数字技术股份有限公司、深圳市蓝凌软件股份有限公司、北京坤豆科技有限公司、北京通达志成科技有限公司、杭州帕拉迪网络科技有限公司、杭州海康威视系统技术有限公司、索尼（中国）有限公司、保定市互动企业营销策划有限公司、青岛易企天创管理咨询有限公司、索尼（中国）有限公司、保定市互动企业营销策划有限公司、青岛易企天创管理咨询有限公司、湖南翱云网络科技有限公司、西安众邦网络科技有限公司、正方软件股份有限公司、深圳市联软科技股份有限公司、友讯电子设备（上海）有限公司、北京伍联维度科技有限公司、烽火通信科技股份有限公司、石家庄市征红网络科技有限公司、浙江大华技术股份有限公司、郑州晨华科技有限公司、重庆名爵科技有限公司、太原迅易科技有限公司、上海普加软件有限公司、北京易网信科技发展有限公司、上海帝联信息科技股份有限公司、杭州世导科技有限公司、上海优刻得信息科技有限公司、杭州世导信息技术有限公司、湖南思智网络科技有限公司、北京创想寰宇网络科技有限公司、北京京宽科技发展有限公司、北京光环新网科技股份有限公司、浙江天猫技术有限公司、中电华通通信有限公司北京分公司、河南亿恩科技股份有限公司、成都西维数码科技有限公司、广州海之光通信技术股份有限公司、西门子（中国）有限公司、北京猎豹移动科技有限公司、腾讯云计算（北京）有限责任公司、阿里巴巴集团、中国知网、京东安全应急响应中心、施耐德（Schneider Electric）、Apache 软件基金会、ZZCMS、YApi、BSP Security、Catfish CMS、6kbbs 和 Memurai。

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、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、长春嘉诚信息技术股份有限公司、山东华鲁科技发展股份有限公司、河南灵创电子科技有限公司、杭州迪普科技股份有限公司、广西启汇壹星信息科技有限公司、京东云安全、山东云天安全技术有限公司、南京众智维信息科技有限公司、星云博创科技有限公司、北京天地和兴科技有限公司、博智安全科技股份有限公司、北京顶象技术有限公司、上海观安信息技

术股份有限公司、河南信安世纪科技有限公司、上海市信息安全测评认证中心、成都愚安科技有限公司、上海犀点意象网络科技有限公司、山石网科通信技术股份有限公司、北京智游网安科技有限公司、清远职业技术学院、北京卓识网安技术股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）及其他个人白帽子向 CNVD 提交了 2152 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）和上海交大向 CNVD 共享的白帽子报送的 1357 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）	639	639
上海交大	493	493
北京神州绿盟科技有限公司	286	2
奇安信网神（补天平台）	225	225
哈尔滨安天科技集团股份有限公司	199	0
华为技术有限公司	180	0
新华三技术有限公司	154	0
北京天融信网络安全技术有限公司	135	14
北京启明星辰信息安全技术有限公司	110	1
深信服科技股份有限公司	98	0
中新网络信息安全股份有限公司	40	40
中国电信集团系统集成有限责任公司	35	35
西安四叶草信息技术有限公司	17	17
北京知道创宇信息技术股份有限公司	6	6
国瑞数码零点实验室	181	181
长春嘉诚信息技术股份有限公司	64	64
山东华鲁科技发展股份有限公司	33	33

河南灵创电子科技有限公司	31	31
杭州迪普科技股份有限公司	16	2
广西启汇壹星信息科技有限公司	11	11
京东云安全	9	9
山东云天安全技术有限公司	8	8
南京众智维信息科技有限公司	7	7
星云博创科技有限公司	7	7
北京天地和兴科技有限公司	4	4
博智安全科技股份有限公司	4	4
北京顶象技术有限公司	4	4
上海观安信息技术股份有限公司	4	4
河南信安世纪科技有限公司	3	3
上海市信息安全测评认证中心	2	2
成都愚安科技有限公司	1	1
上海犀点意象网络科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京智游网安科技有限公司	1	1
清远职业技术学院	1	1
北京卓识网安技术股份有限公司	1	1
北京云科安信科技有限公司（Seraph 安全实验室）	1	1
CNCERT 四川分中心	1	1
个人	298	298

报送总计	3311	2152

本周漏洞按类型和厂商统计

本周，CNVD 收录了 395 个漏洞。应用程序 222 个，WEB 应用 65 个，操作系统 63 个，网络设备（交换机、路由器等网络端设备）21 个，智能设备（物联网终端设备）15 个，安全产品 8 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	222
WEB 应用	65
操作系统	63
网络设备（交换机、路由器等网络端设备）	21
智能设备（物联网终端设备）	15
安全产品	8
数据库	1

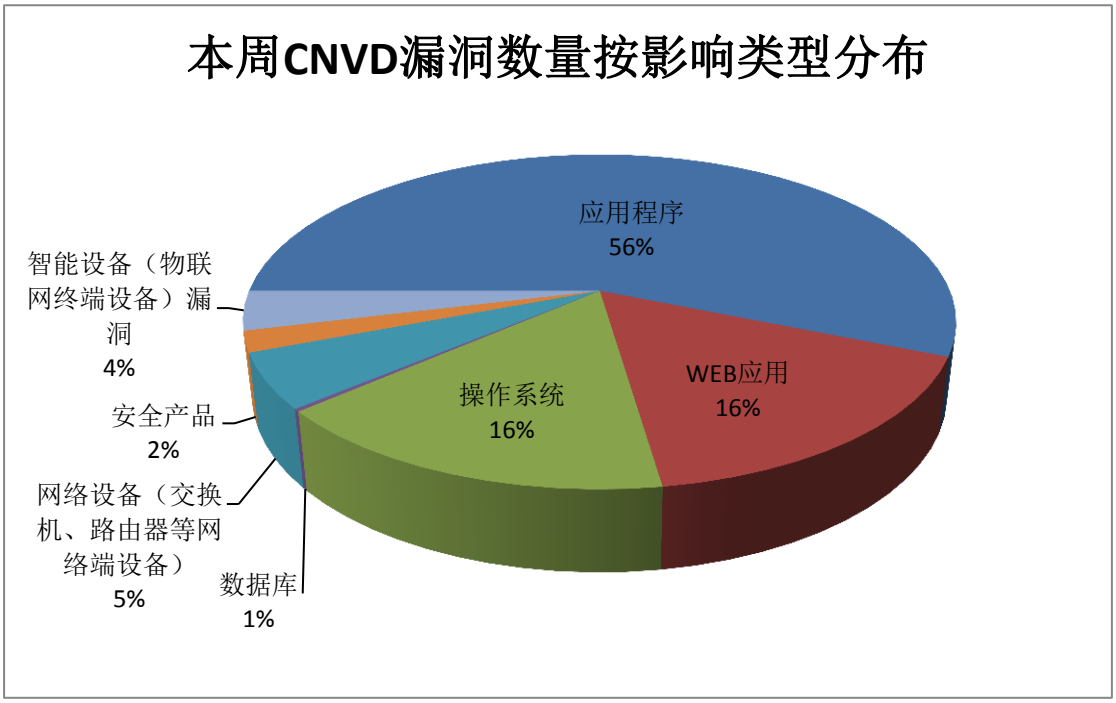

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Adobe、Mcafee 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	Oracle	29	7%
2	Adobe	24	6%
3	Mcafee	22	6%
4	Microsoft	21	5%
5	Huawei	18	5%
6	IBM	16	4%
7	Linux	16	4%
8	CloudBees	14	4%
9	Mattermost	11	3%
10	其他	224	56%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，15 个移动互联网行业漏洞，15 个工控行业漏洞（如下图所示）。其中，“多款 Apple 产品 Python 组件内存损坏漏洞、Philips Clinical Collaboration Platform 访问控制不当漏洞”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/

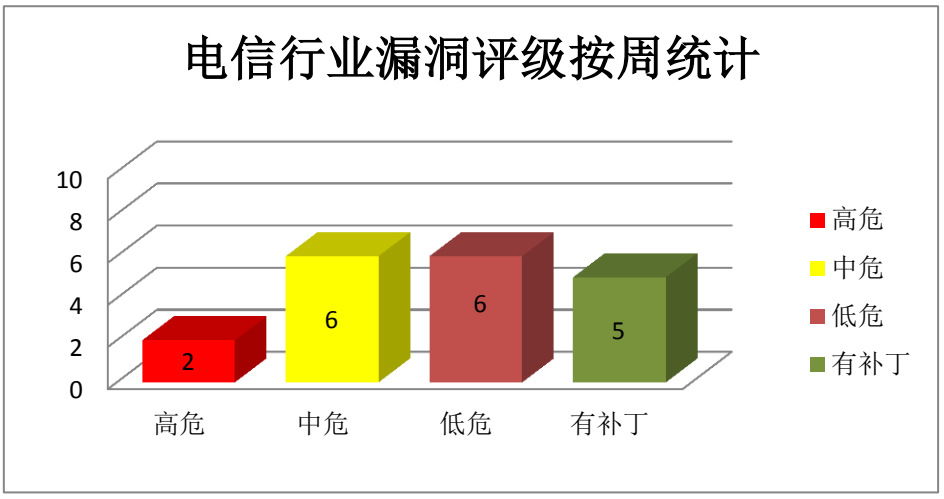

图 3 电信行业漏洞统计

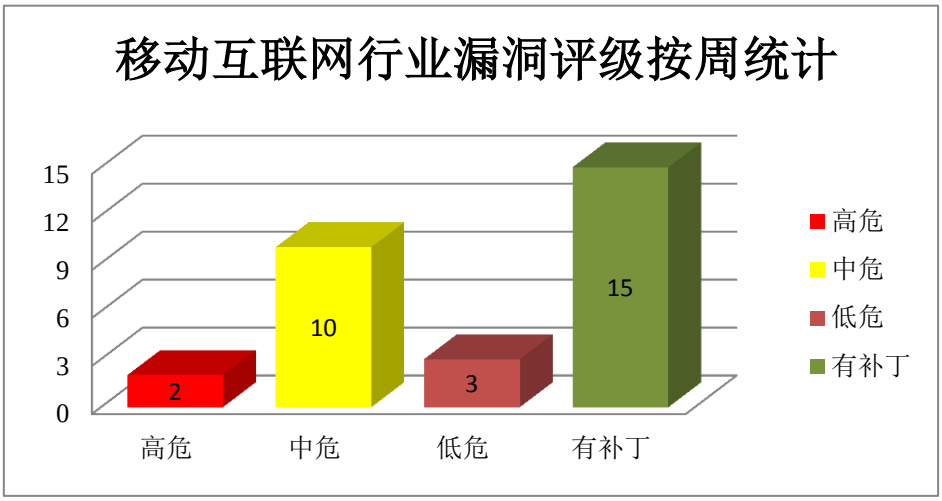

图 4 移动互联网行业漏洞统计

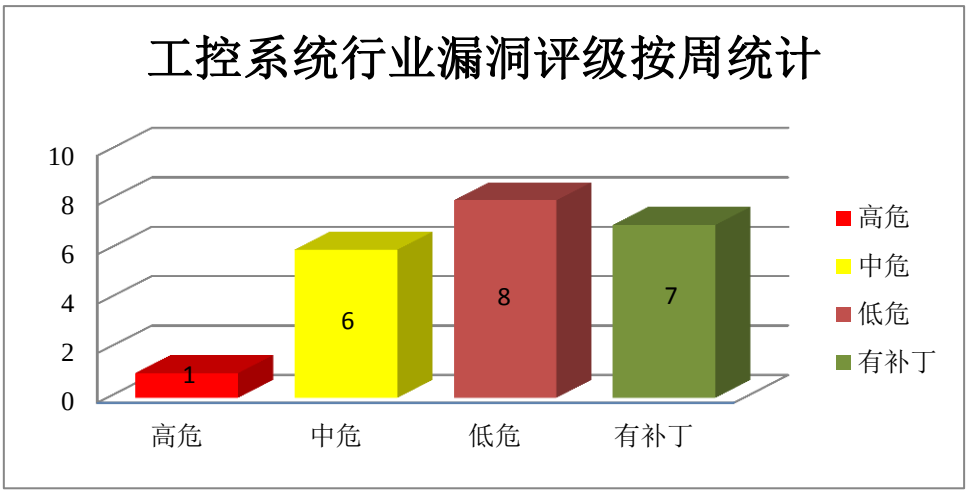

图 5 工控系统行业漏洞统计

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、 McAfee 产品安全漏洞

McAfee Data Loss Prevention Endpoint（DLPe）是美国迈克菲（McAfee）公司的一套集成式终端数据保护解决方案。McAfee Web Gateway 是高性能安全 Web 网关，采用一个统一的设备软件架构,具有同类最佳的威胁防护。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 Windows 锁屏，访问受保护的配置文件，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：McAfee Data Loss Prevention Endpoint 缓冲区溢出漏洞（CNVD-2020-51803、CNVD-2020-51804）、McAfee Data Loss Prevention Endpoint 身份验证绕过漏洞、McAfee Web Gateway 权限提升漏洞（CNVD-2020-52201、CNVD-2020-52202、CNVD-2020-52200、CNVD-2020-52199、CNVD-2020-52198）。其中，“M

cAfee Web Gateway 权限提升漏洞（CNVD-2020-52198）”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-2020-51804
https://www.cnvd.org.cn/flaw/show/CNVD-2020-51803
https://www.cnvd.org.cn/flaw/show/CNVD-2020-51808
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52201
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52200
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52199
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52198
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52202

2、Microsoft 产品安全漏洞

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。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：Microsoft Windows Kernel 权限提升漏洞（CNVD-2020-52072、CNVD-2020-52077）、Microsoft Windows Function Discovery SSDP 权限提升漏洞、Microsoft Windows dnsrslvr.dll 权限提升漏洞、Microsoft Windows Ancillary Function Driver for WinSock 权限提升漏洞、Microsoft Windows Jet Database Engine 远程代码执行漏洞（CNVD-2020-52085、CNVD-2020-52084、CNVD-2020-52086）。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-2020-52072
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52071
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52078
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52077
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52082
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52085
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52084
https://www.cnvd.org.cn/flaw/show/CNVD-2020-52086

3、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 都是美国奥多比（Adobe）公司的产品。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Reader 是一套 PDF 文档阅读软件。Adobe Magento 是一套开源的 PHP 电子商务系统。本周，上述产品被披露存在多个漏洞，攻击者可利用

漏洞绕过身份验证，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Magento 身份验证绕过漏洞、Adobe Acrobat 和 Reader 内存破坏漏洞（CNVD-2020-52166、CNVD-2020-52168）、Adobe Acrobat 和 Reader 类型混淆漏洞（CNVD-2020-52170、CNVD-2020-52173、CNVD-2020-52172、CNVD-2020-52171）、Adobe Magento Open Source 和 Magento Commerce 代码注入漏洞。其中，“Adobe Acrobat 和 Reader 内存破坏漏洞（CNVD-2020-52166、CNVD-2020-52168）、Adobe Magento 身份验证绕过漏洞、Adobe Magento Open Source 和 Magento Commerce 代码注入漏洞”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-2020-52166

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52165

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52168

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52170

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52173

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52172

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52171

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52852

4、IBM 产品安全漏洞

IBM Blade Center 是一款 IBM 的服务器管理程序。IBM Maximo Asset Management 是一套综合性资产生命周期和维护管理解决方案。IBM Spectrum Protect Plus 是一套数据保护平台。IBM Spectrum Protect 是一套数据保护平台。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，访问受限目录之外的位置，在目标用户上下文执行恶意操作，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM BladeCenter 跨站请求伪造漏洞（CNVD-2020-52190、CNVD-2020-52615）、IBM Maximo Asset Management 跨站请求伪造漏洞（CNVD-2020-52459）、IBM Maximo Asset Management 反向标签劫持漏洞、IBM Maximo Asset Management 代码执行漏洞、IBM Maximo Asset Management SQL 注入漏洞（CNVD-2020-52460）、IBM Spectrum Protect Plus 路径遍历漏洞（CNVD-2020-52458、CNVD-2020-52457）。其中“IBM Maximo Asset Management 代码执行漏洞、IBM BladeCenter 跨站请求伪造漏洞”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-2020-52190

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52459

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52458

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52457

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52461

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52460

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52615

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52614

5、NVIDIA Linux GPU Display Driver 竞争条件问题漏洞

NVIDIA Linux GPU Display Driver 是美国英伟达（NVIDIA）公司的一款专用于 Linux 平台的图形处理器（GPU）显卡驱动程序。本周，NVIDIA Linux GPU Display Driver 产品被披露存在竞争条件问题漏洞。攻击者可利用该漏洞造成拒绝服务。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-2020-52627

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-2020-51792	Apache ActiveMQ 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：http://activemq.apache.org/security-advisories.data/CVE-2020-11998-announcement.txt
CNVD-2020-51797	F5 BIG-IP 访问控制错误漏洞（CNVD-2020-51797）	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/K91158923?utm_source=f5support&utm;_medium=RSS
CNVD-2020-51806	Cisco IP Phone 8800 Series 和 Cisco IP Phone 7800 Series 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190703-ip-phone-sip-dos
CNVD-2020-52187	Palo Alto Networks PAN-OS 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://security.paloaltonetworks.com/CVE-2020-2037
CNVD-2020-52197	Trend Micro Apex One 权限提升漏洞	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/000263632
CNVD-2020-52338	Ingenico Telium 2 POS 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://ingenico.us/smart-terminals/telium2
CNVD-2020-52376	D-Link DCS-2530L 和 DCS-2670L 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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10180
CNVD-2020-52625	Xen Linux kernel 权限控制漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=cadfad870154e14f745ec845708bc17d166065f2
CNVD-2020-52631	Nitro Software Nitro Pro 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.gonitro.com/nps/product-details/downloads
CNVD-2020-52878	SpamTitan 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.spamtitan.com/

小结：本周，McAfee 产品被披露存在多个漏洞，攻击者可利用漏洞绕过 Windows 锁屏，访问受保护的配置文件，导致缓冲区溢出或堆溢出等。此外，Microsoft、Adobe、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证，获取敏感信息，提升权限，执行任意代码等。另外，NVIDIA Linux GPU Display Driver 产品被披露存在竞争条件问题漏洞。攻击者可利用该漏洞造成拒绝服务。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、Linux expand_downwards()竞争条件漏洞

验证描述

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。

Linux expand_downwards()存在竞争条件漏洞。攻击者可借助特制的请求利用该漏洞造成拒绝服务。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2020090074

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-52617

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. 美国土安全部发出罕见紧急警告：Windows 存在“严重”漏洞

在最近披露微软 Windows 服务器版本存在“严重”安全漏洞后，美国土安全部网络安全顾问组罕见地向政府部门发布了紧急警报。CISA 要求所有联邦部门和机构立即对任何容易受到 Zerologon 攻击的 Windows 服务器进行补丁，称这对政府网络构成了不可接受的风险。

参考链接：https://www.cnbeta.com/articles/tech/1031235.htm

2. Adobe 发布了带外安全更新，以修复三个严重漏洞

Adobe 发布了带外安全更新，以解决 Adobe Media Encoder 中的三个“严重”的安全漏洞。攻击者可以利用这三个漏洞来访问在用户泄露的敏感信息。

参考链接：https://securityaffairs.co/wordpress/108329/security/adobe-media-encoder-flaws.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