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 21 日-2020 年 09 月 27 日　　2020 年第 39 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 369 个，其中高危漏洞 68 个、中危漏洞 239 个、低危漏洞 62 个。漏洞平均分值为 5.21。本周收录的漏洞中，涉及 0day 漏洞 109 个（占 30%），其中互联网上出现“Anchor CMS 存储型跨站脚本漏洞、BigTree CMS 远程执行代码漏洞”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 2902 个，与上周（2152 个）环比增加 35%。

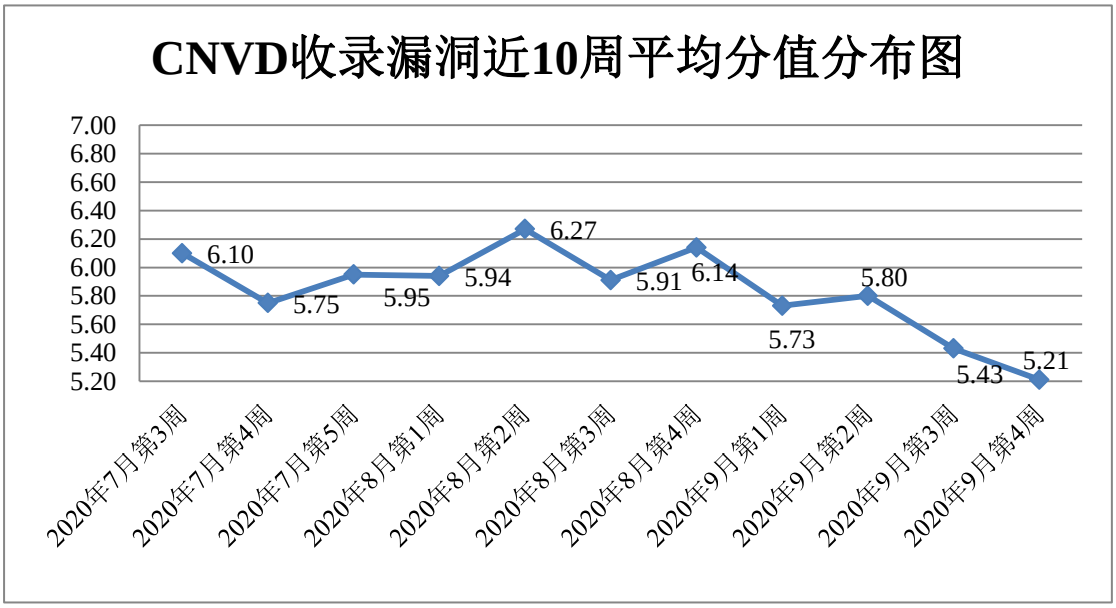

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 起，向基础电信企业通报漏洞事件 12 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 273 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 28 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、南京庞特软件科技有限公司、上海泛微网络科技股份有限公司、杭州当贝网络科技有限公司、微软(中国)有限公司、石家庄市征红网络科技有限公司、上海瑞策软件有限公司、深圳艾维信息有限公司、杭州安恒信息技术股份有限公司、南通艾睦网络科技有限公司、瑞芯微电子股份有限公司、西门子（中国）有限公司、广州齐博网络科技有限公司、深圳市福洽科技有限公司、苏州汇川技术有限公司、深圳市捷顺科技实业股份有限公司、澳门软通动力科技有限公司、佛山市铁马软件有限公司、微星科技股份有限公司、欧姆龙（中国）有限公司、合肥彼岸互联信息技术有限公司、北京通达志成科技有限公司、施耐德电气（中国）有限公司、西安佰联网络技术有限公司、上海商派网络科技有限公司、郑州微口网络科技有限公司、科大讯飞股份有限公司、武汉创益云信息技术有限公司、西安九佳易信息资讯有限公司、深圳市迅雷网文化有限公司、上海起迪计算机科技发展有限公司、欧姆龙自动化（中国）有限公司、北京中星微电子有限公司、江苏固德威电源科技股份有限公司、河南青峰网络科技有限公司、青岛易企天创管理咨询有限公司、西安网卓信息技术有限公司、北京中成科信科技发展有限公司、北京人大金仓信息技术股份有限公司、北京致远互联软件股份有限公司、深圳市宜搜科技发展有限公司、新乡市大邦计算机软件有限公司、华硕电脑（上海）有限公司、深圳市瑞吉联通信科技有限公司、杭州海康威视系统技术有限公司、深圳极速创想科技有限公司、北京金山安全管理系统技术有限公司、北京通达信科科技有限公司、拍旁科技、天途 CMS、6KBBS、Mitsubishi Electric Corporation、GENEXIS、Excitel、Catfish CMS 、Mkvalidator、UCMS、Zzzcms、Tycoding、Syrotech、Technxt、PCFCMS 和 ZZCMS。

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、北京神州绿盟科技有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司、华为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、山东新潮信息技术有限公司、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、长春嘉诚信息技术股份有限公司、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、北京网御星云信息技术有限公司、安徽长泰信息安全服务有限公司、河南信安世纪科技有限公司、北京顶象技术有限公司、北京天地和兴科技有限公司、杭州海康威视数字技术股份有限公司、浙江安腾信息技术有限公司、国家电网公司、广西塔易

信息技术有限公司、上海市信息安全测评认证中心、北京云科安信科技有限公司（Seraph安全实验室）、广州安亿信软件科技有限公司、广州市云聚数据服务有限公司、中科信息安全共性技术国家工程研究中心有限公司、深圳市魔方安全科技有限公司、北京智游网安科技有限公司及其他个人白帽子向 CNVD 提交了 2902 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 1809 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）	1036	1036
上海交大	428	428
奇安信网神（补天平台）	345	345
哈尔滨安天科技集团股份有限公司	242	0
北京神州绿盟科技有限公司	206	6
新华三技术有限公司	173	0
北京天融信网络安全技术有限公司	163	4
华为技术有限公司	147	0
中新网络信息安全股份有限公司	139	139
北京启明星辰信息安全技术有限公司	120	6
深信服科技股份有限公司	101	0
北京奇虎科技有限公司	31	31
中国电信集团系统集成有限责任公司	9	9
恒安嘉新(北京)科技股份公司	4	0
北京知道创宇信息技术股份有限公司	2	0
国瑞数码零点实验室	190	190
山东新潮信息技术有限公司	92	92

山东华鲁科技发展股份有限公司	62	62
河南灵创电子科技有限公司	28	28
长春嘉诚信息技术股份有限公司	22	22
杭州迪普科技股份有限公司	15	0
京东云安全	15	15
山东云天安全技术有限公司	15	15
南京众智维信息科技有限公司	14	14
北京网御星云信息技术有限公司	13	13
安徽长泰信息安全服务有限公司	10	10
河南信安世纪科技有限公司	10	10
北京顶象技术有限公司	10	10
北京天地和兴科技有限公司	8	8
杭州海康威视数字技术股份有限公司	8	8
浙江安腾信息技术有限公司	5	5
国家电网公司	4	4
广西塔易信息技术有限公司	3	3
上海市信息安全测评认证中心	2	2
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
广州安亿信软件科技有限公司	1	1
广州市云聚数据服务有限公司	1	1
中科信息安全共性技术国家工程研究中心有限公司	1	1
深圳市魔方安全科技有限公司	1	1

北京智游网安科技有限公司	1	1
CNCERT 海南分中心	12	12
CNCERT 青海分中心	4	4
CNCERT 四川分中心	3	3
CNCERT 天津分中心	1	1
CNCERT 山东分中心	1	1
CNCERT 河北分中心	1	1
个人	358	358
报送总计	4059	2902

本周漏洞按类型和厂商统计

本周，CNVD 收录了 369 个漏洞。应用程序 176 个，WEB 应用 76 个，操作系统 73 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）11 个，安全产品 11 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	176
WEB 应用	76
操作系统	73
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）	11
安全产品	11
数据库	1

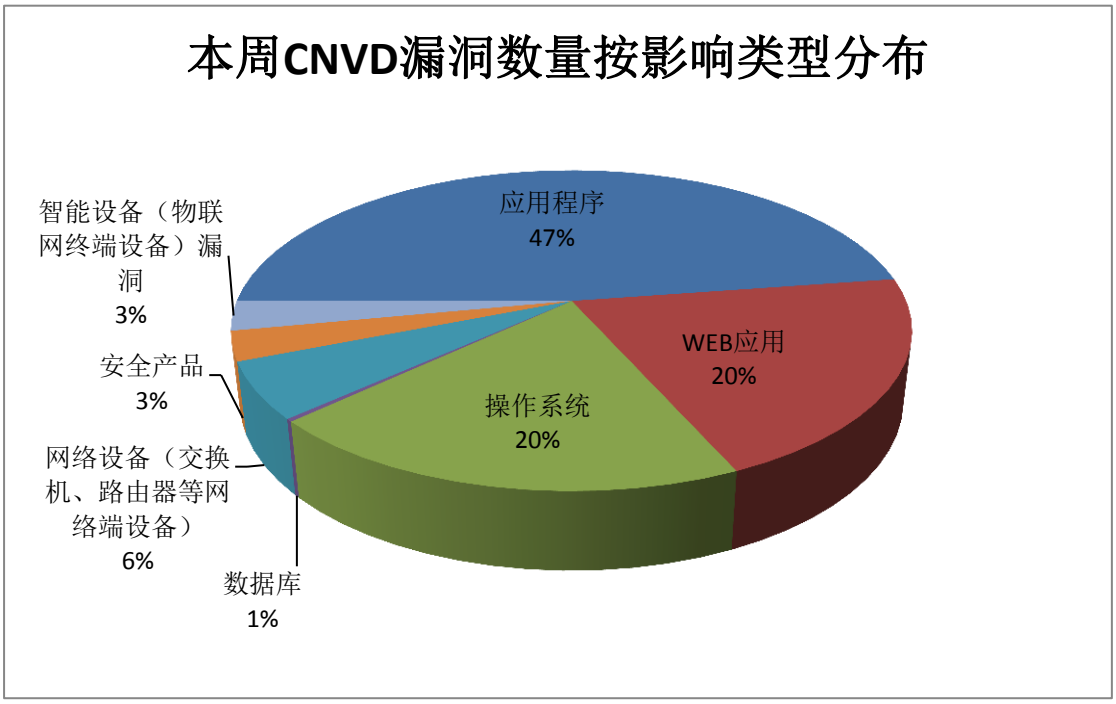

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、SAP 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	Google	58	15%
2	Microsoft	32	9%
3	SAP	22	6%
4	Atlassian	16	4%
5	IBM	15	4%
6	Mcafee	14	4%
7	小米科技有限责任公司	13	4%
8	Joomla!	10	3%
9	Gradle	8	2%
10	其他	181	49%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，56 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“EdgeSwitch 命令注入漏洞、Xiaomi router 输入验证错误

漏洞、Google Android 权限提升漏洞（CNVD-2020-53775）、Advantech iView 路径遍历漏洞”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/

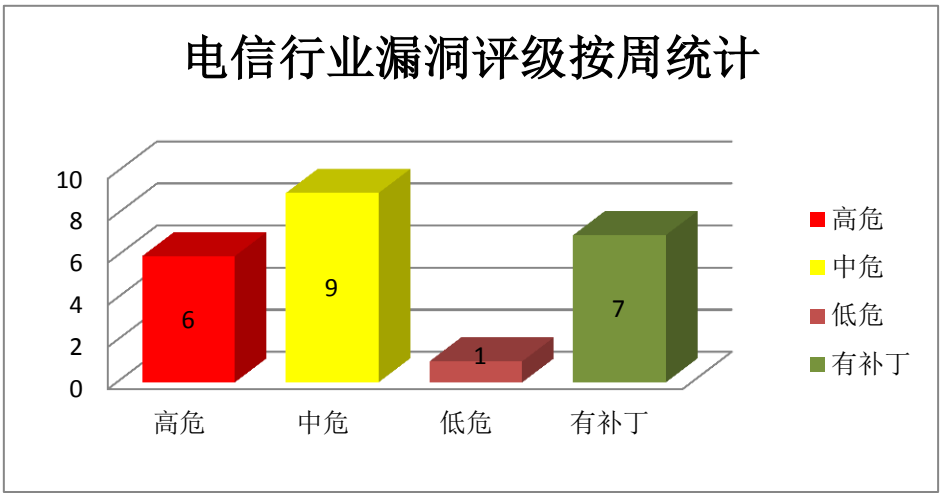

图 3 电信行业漏洞统计

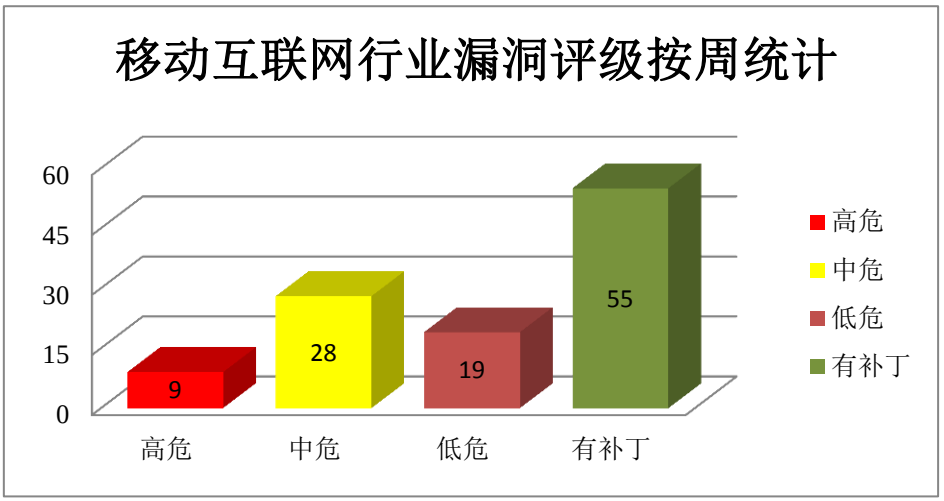

图 4 移动互联网行业漏洞统计

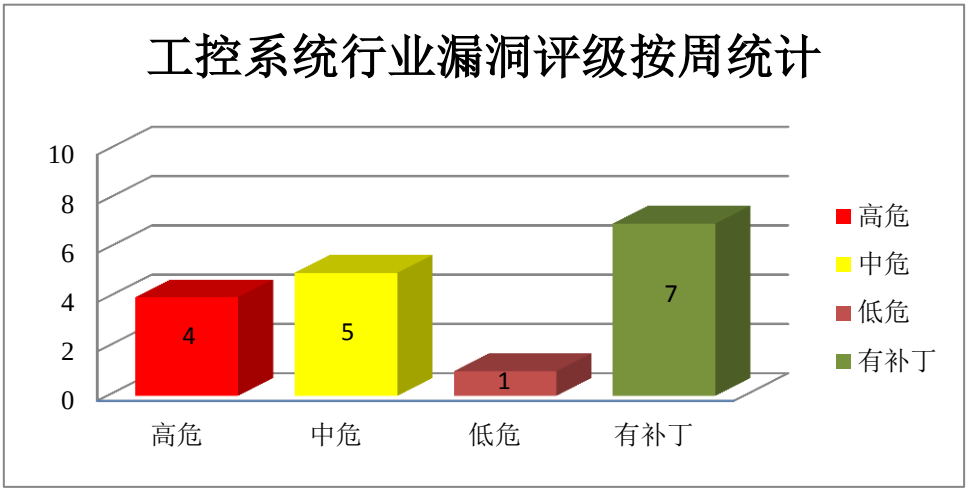

图 5 工控系统行业漏洞统计

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 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权限提升漏洞，攻击者可利用漏洞以提升的权限执行代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Print Workflow Service 权限提升漏洞、Microsoft Windows Error Reporting Manager 权限提升漏洞（CNVD-2020-52921）、Microsoft Windows Network Location Awareness Service 权限提升漏洞、Microsoft Windows Sync Host Service 权限提升漏洞、Microsoft Windows UPnP 权限提升漏洞、Microsoft Windows ActiveX Installer Service 权限提升漏洞（CNVD-2020-52928）、Microsoft Windows AppX Deployment Extensions 权限提升漏洞、Microsoft Windows Function Discovery Service 权限提升漏洞。其中，“Microsoft Windows Error Reporting Manager 权限提升漏洞（CNVD-2020-52921）、Microsoft Windows ActiveX Installer Service 权限提升漏洞（CNVD-2020-52928）”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-2020-52910

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52921

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52920

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52919

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52922

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52928

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52926

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52929

2、Atlassian 产品安全漏洞

Atlassian JIRA Server 是一套缺陷跟踪管理系统的服务器版本。Atlassian JIRA Data Center 是 Atlassian JIRA 的数据中心版本。Atlassian Confluence Server 是澳大利亚 Atlassian 公司的一套专业的企业知识管理与协同软件，也可以用于构建企业 WiKi。Atlassian Fisheye 是一套源代码深度查看软件。Crucible 是一套代码审查工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行未授权的操作，获取敏感信息，注入任意 HTML 或 JavaScript，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Atlassian Jira 信息泄露漏洞（CNVD-2020-52940）、Atlassian JIRA Server 和 Data Center 跨站请求伪造漏洞、Atlassian Confluence Server 跨站脚本漏洞（CNVD-2020-52943）、Atlassian Fisheye 和 Crucible 未授权操作漏洞、Atlassian JIRA Server 和 Data Center 注入漏洞、Atlassian JIRA Server 和 Data Center 拒绝服务漏洞（CNVD-2020-53361）、Atlassian JIRA Server 和 Data Center 跨站脚本漏洞（CNVD-2020-53363、CNVD-2020-53362）。其中，“Atlassian JIRA Server 和 Data Center 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-2020-52940

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52944

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52943

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52948

https://www.cnvd.org.cn/flaw/show/CNVD-2020-52946

https://www.cnvd.org.cn/flaw/show/CNVD-2020-53361

https://www.cnvd.org.cn/flaw/show/CNVD-2020-53363

https://www.cnvd.org.cn/flaw/show/CNVD-2020-53362

3、Google 产品安全漏洞

Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）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权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Telephony 权限提升漏洞（CNVD-2020-53138）、Google Android 权限提升漏洞（CNVD-2020-53763、CNVD-2020-53768、CNVD-2020-53769、CNVD-2020-53774、CNVD-2020-53775）、Google Android Kernel 组件权限提升漏洞（CNVD-2020-54064）、Google Android Framework 权限提升漏洞（CNVD-2020-54072）。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-2020-53138
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53763
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53768
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53769
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53774
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53775
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54064
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54072

4、McAfee 产品安全漏洞

McAfee Agent（MA）是一套提供了 ePolicy Orchestrator（杀毒软件管理平台）与被管理产品之间的安全通信的客户端组件。McAfee Host Intrusion Prevention System（Host IPS）是一套主机入侵防御系统。McAfee Total Protection（MTP）是一套防病毒软件。McAfee Email Gateway（MEG）是一套电子邮件安全解决方案。McAfee VirusScan Enterprise（VSE）是一套杀毒软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未授权删除文件，执行任意代码等。

CNVD 收录的相关漏洞包括：McAfee Agent 代码问题漏洞、McAfee Host Intrusion Prevention System 代码问题漏洞、McAfee VirusScan Enterprise 权限许可和访问控制问题漏洞、McAfee Total Protection 权限提升漏洞（CNVD-2020-53311、CNVD-2020-54153）、McAfee Email Gateway 路径遍历漏洞、McAfee Total Protection MTP Free Antivirus Trial 代码问题漏洞、McAfee Agent 权限提升漏洞。其中“McAfee VirusScan Enterprise 权限许可和访问控制问题漏洞”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-2020-53123
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53291
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53290
https://www.cnvd.org.cn/flaw/show/CNVD-2020-53311
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54148
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54155
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54153
https://www.cnvd.org.cn/flaw/show/CNVD-2020-54156

5、3S-Smart Software Solutions CODESYS Runtime 远程代码执行漏洞

3S-Smart Software Solutions CODESYS Runtime 是一套基于 IEC61131-3 标准编程的控制器实时运行系统。本周，3S-Smart Software Solutions CODESYS Runtime 被披露存在远程代码执行漏洞。攻击者可通过发送恶意的数据包利用该漏洞执行代码。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-2020-53804

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-2020-53115	Trustwave MailMarshal 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www3.trustwave.com/software/mailmarshal_smtp/mailmarshalseg-releasenotes-7.2.0.6272.htm
CNVD-2020-53120	Meetecho Janus 缓冲区溢出漏洞（CNVD-2020-53120）	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/meetecho/janus-gateway/pull/2229
CNVD-2020-53119	Meetecho Janus 缓冲区溢出漏洞（CNVD-2020-53119）	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/meetecho/janus-gateway/pull/2229
CNVD-2020-53525	Micro Focus Operations Bridge Reporter 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://softwaresupport.softwaregrp.com/doc/KM03710590
CNVD-2020-53781	Xiaomi router 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=20&locale;=en
CNVD-2020-53783	Sagemcom F@ST 5280 routers 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://seclists.org/fulldisclosure/2020/Sep/3
CNVD-2020-53785	EdgeSwitch 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://www.ui.com/download/edgemax/
CNVD-2020-53798	ASUS Aura Sync 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.asus.com.cn/
CNVD-2020-53815	Xen 拒绝服务漏洞（CNVD-2020-53815）	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://xenbits.xen.org/xsa/advisory-343.html
CNVD-2020-54082	Teclib GLPI SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/glpi-project/glpi/commit/684d4fc423652ec7dde21cac4d41c2df53f56b3c

小结：本周，Microsoft 产品被披露存在权限提升漏洞，攻击者可利用漏洞以提升的权限执行代码。此外，Atlassian、Google、McAfee 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行未授权的操作，获取敏感信息，提升权限，执行任意代码，发起拒绝服务攻击等。另外，3S-Smart Software Solutions CODESYS Runtime 被披露存在远程代码执行漏洞。攻击者可通过发送恶意的数据包利用该漏洞执行代码。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、BigTree CMS 远程执行代码漏洞

验证描述

BigTree CMS 是一个基于 PHP 和 Mysql 的小型开源 cms。

BigTree CMS 存在远程执行代码漏洞。攻击者可利用漏洞执行任意代码。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=36187

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-54147

信息提供者

CNVD 工作组

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. Instagram 的漏洞可以让黑客远程访问设备

Facebook 已经解决了 Instagram 中的一个严重漏洞，该漏洞该导致智能手机摄像头，麦克风等被劫持，然后远程执行代码。该漏洞由 Check Point 发现，称为 CVE-2020-1895，是 Instagram 图像处理中的一个堆溢出问题，其 CVSS 评分为 7.8。

参考链接：https://securityaffairs.co/wordpress/108709/hacking/instagram-rce-flaw.html

2. 韩国办公处理软件 HanSoft Office 缓冲区溢出漏洞

Hancom 公司为韩国的政府所支持的软件公司。目前主要的是两个产品系列，一个是 Hancom Office，另一个是 ThinkFree Office。Hancom Office 套件里主要包含 HanCell（类似微软的 Excel），HanShow （类似微软的 PowerPoint），HanWord（也就是 HWP，类似微软的 Office Word）等。当 Hancom Office 在处理畸形的 hwp 文件格式时，发生空指针引用，从而造成程序崩溃。

参考链接：https://www.freebuf.com/vuls/250806.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